Estudo Técnico Preliminar 1/2021

1. Informações Básicas

Número do processo: 02001.005149/2020-52

2. Descrição da necessidade

2.1 **Necessidade da Contratação**

2.1.1 A segurança da rede do Ibama 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.

2.1.2 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 por ventura ocorrer no âmbito da rede do Ibama, tendo como alvo ou mesmo vetor de contaminação e execução um dos equipamentos plugados na rede.

2.1.3 De acordo com o último levantamento o Ibama possui um amplo parque computacional para atendimento aos usuários, sem contar os equipamentos que estão para serem recebidos e atualizarão/substituirão esse parque.

2.1.4 O parque de servidores, o Ibama está em processo de migração de serviços hospedados em sua sala-segura para o Serpro, então, até que o processo esteja concluído, é necessário que os servidores de rede estejam plenamente protegidos.

2.1.5 As fontes de contaminação por pragas digitais vão desde a invasão da rede por um elemento mal intencionada, que explora vulnerabilidades de rede e computadores, até o próprio comportamento do usuário do Ibama, 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.

2.1.6 Desta forma, faz-se necessário prover o Ibama 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.

2.1.7 A ferramenta atual de antivírus do Ibama está desatualizada e impede que até mesmo recursos de Sistemas Operacionais mais recentes sejam utilizados, o que aumenta o potencial de invasão contra a rede do Ibama.

2.1.8 Necessidades de negócio

- Os serviços de Tecnologia da Informação prestados pelo Ibama precisam estar disponíveis
- Os serviços de Tecnologia da Informação prestados pelo Ibama precisam estar Íntegros
- Os serviços de Tecnologia da Informação prestados pelo Ibama precisam estar Confiáveis
- O processo de fiscalização ambiental requer que os recursos de Tecnologia da Informação estejam operantes
- O processo de controle e transporte de cargas perigosas requer que os recursos de Tecnologia da Informação estejam operantes
- O processo de controle da qualidade ambiental requer que os recursos de Tecnologia da Informação estejam operantes
- O processo de licenciamento ambiental requer que os recursos de Tecnologia da Informação estejam operantes

2.1.9 Necessidades tecnológicas

- Aquisição de ferramentas atuais para o tratamento dos incidentes de segurança da informação
- Manutenção de atualização das licenças e dos recursos de prevenção para detecção e atuação em caso de incidentes de segurança da informação
- Suporte contínuo e especializado ao corpo técnico de gestão do Ibama para o tratamento e prevenção dos incidentes de segurança da informação

3. Área requisitante

Área Requisitante	Responsável
Coordenação de Infraestrutura Tecnológica	Cleiton Araújo de Oliveira

4. Descrição dos Requisitos da Contratação

4 **Demais requisitos necessários e suficientes à escolha da solução de TIC**

4.1 Requisitos de Negócio

- 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.
- Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e repasse de conhecimento, conforme detalhado no item console de gerência: 6.5.
- Garantia da solução pelo prazo de 12 (doze) meses, na forma do item 4.4.
- 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.
- 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”).

4.2 **Requisitos de Capacitação**

- A Contratada deverá realizar o repasse de conhecimento da solução que está sendo fornecida.

4.3 **Requisitos Legais**

- Lei n° 8.666, de 21 de junho de 1993, que institui normas para licitações e Contratos da Administração Pública.
- 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.
- 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.
- Lei n° 8.248, de 23 de outubro de 1991, que dispõe sobre a capacitação e competitividade do setor de informática e automação.
- 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.
- 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.
- Decreto lei 9.760/2019, de 11 de abril de 2019, que alterou o Decreto nº 6.514, de 22 de julho de 2008.
- 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”.
- 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.
- Não haverá incidência de margem de preferência prevista no Decreto nº 8.186, de 17 de janeiro de 2014, que “Estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de licenciamento de uso de programas de computador e serviços correlatos, para fins do disposto no art. 3º da Lei nº 8.666, de 21 de junho de 1993”, visto que a presente licitação não é voltada para empresas desenvolvedoras de software, e sim para empresas que comercializam equipamentos, as quais não recebem o certificado previsto no art. 2º, II,do Decreto nº 8.186, de 17 de janeiro de 2014.

- 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.
- 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.

4.4 **Requisitos de Manutenção**

- A Contratada deverá fornecer garantia da solução pelo prazo de 12 (doze) meses, contados a partir da data da emissão do Termo de Recebimento, não se limitando ao término da vigência contratual.
- Deverá ser oferecido suporte da Contratada, com possibilidade de abertura de chamados em regime de 12x5, de 8h00 às 20h00, nos dias comerciais, para resolução de problemas.
- 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.
- Deverá ser fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimentos e a fóruns sobre a solução.
- 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;
    - A garantia deverá ser prestada durante todo o período de contrato e aditivos relativos as a atualização das licenças e proteção.
- As manutenções corretivas, por solicitação expressa do Ibama à Contratada, e preventiva, por solicitação da Contratada ao Ibama, serão realizadas dentro dos seguintes limites:
    - No caso de manutenções preventivas, o horário do atendimento deverá ser compreendido entre 9h00 e 18h00, em dias úteis (5 x 9h);
    - No caso de manutenções corretivas, o horário do atendimento deverá ser compreendido entre 8h00 e 20h00, em dias úteis (5 x 12h);

4.5 Requisitos Temporais

- Na contagem dos prazos estabelecidos neste Termo de Referência, quando não expressados de forma contrária, excluir-se-á o dia do início e incluir-se-á o do vencimento.
- Todos os prazos citados, quando não expresso de forma contrária, serão considerados em dias corridos (ou horas corridas, quando definido em horas).
- Todos os eventos de trabalho que envolva participação de integrantes da CONTRATANTE e/ou órgãos de governo serão realizadas de segunda-feira a sexta-feira das 08:00 às 18:00, exceto feriados.
- Todos os eventos de trabalho que envolva participação de integrantes da CONTRATADA em ambiente da CONTRATANTE serão realizadas de segunda-feira a sexta-feira das 08:00 às 18:00, exceto feriados, salvo acordo entre as partes.
- 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 Ordem.
- 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.
- 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.
- 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.
- A CONTRATADA deverá disponibilizar, os bens no local indicado e no prazo especificado quando da emissão da Ordem de Serviço de fornecimento.
- Os atendimentos de suporte e assistência técnica devem ser prestados em local a ser indicado pela CONTRATADA nas capitais dos estados da federação, inclusive os de substituição de equipamentos quando necessário por motivo de defeito de fabricação.

4.5 **Requisitos de Segurança e privacidade**

- 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 Ibama, conforme modelo apresentado no ANEXO A - TERMO DE COMPROMISSO. 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.

- 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.
- 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.
- A CONTRATADA obriga-se a dar ciência à CONTRATANTE, imediatamente e por escrito, sobre qualquer anormalidade que verificar na prestação dos serviços.
- 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.
- 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.
- Os equipamentos deverão possuir acesso às correções disponibilizadas pelo fabricante, enquanto existir o suporte às versões fornecidas.

4.6 **Requisitos sociais, ambientais e culturais**

- Quanto aos requisitos sociais, os profissionais da CONTRATADA, quando nas dependências do Ibama, deverão apresentar-se vestido de forma adequada ao ambiente de trabalho, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional do Ibama.
- Os profissionais também deverão respeitar todos os servidores, funcionários e colaboradores em qualquer posição hierárquica, preservando a comunicação e o relacionamento interpessoal construtivo.
- Não aplicação da Instrução Normativa SLTI/MP nº 01, de 19 de janeiro de 2010 - que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional pelo fato de ser tratar de contratação de licenças de software e de serviços especializados.

5. Levantamento de Mercado

5.1 **Alternativas de mercado**

5.1.1 A Contratação como serviço em nuvem de uma solução de proteção contra ameaças avançadas (Next Generation Antivírus - NGAV) baseada em agente com funcionalidade de EDR (“Endpoint Detection and Response”) pode ser atendida por vários fabricantes de mercado tais como: Kaspersky, SentinelOne, CrowdStrike, Antivírus do Windows Defender, Proteção Avançada contra Ameaças do Windows Defender, McAfee Endpoint Security, McAfee Endpoint Protection Suite (Legacy), Sophos Intercept X, Sophos Endpoint Protection, ESET Endpoint Security, Symantec Endpoint Protection, Malwarebytes Endpoint Protection, Anti-Malware for Business (Legacy), Bitdefender Gravityzone Enterprise Security, GravityZone Ultra, GravityZone Elite, GravityZone Business Security, GravityZone Advanced Business Security, VMware Carbon Black Cloud, FortiClient, FortiEDR, Panda Adaptive Defense 360, Panda Endpoint Protection, Panda Endpoint Protection Plus, Trend Micro Apex One, BlackBerry Protect, F-Secure Protection Service for Business, F-Secure Client Security, Instinto profundo(Deep Instict), Cybereason Defense Platform, Check Point SandBlast Agent, Cisco Advance Malware Protection (AMP), FireEye Endpoint Security (HX), Paloalto Cortex XDR, Acronis Cyber Protect.

5.1.2 As informações acima foram obtidas no endereço "https://www.gartner.com/reviews/market/endpoint-protection-platforms/vendors", de acesso público na intenet.

6. Descrição da solução como um todo

6.1 **Solução**

6.1.1 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”).

6.2 **Requisitos gerais da solução:**

6.2.1 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.

6.2.2 Fornecimento da console de gerência, incluindo implantação dos agentes, documentação da arquitetura da solução e repasse de conhecimento, conforme detalhado no item console de gerência: **6.5.**

6.2.3 Garantia da solução pelo prazo de 12 (doze) meses, na forma do item **6.8.**

6.2.4 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.

6.2.5 A solução de proteção deve ser oferecida na última versão disponibilizada pelo fabricante.

6.2.6 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”).

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 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 MITRE ATT&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. Deve ser possível gerar relatório dessas informações.

6.3.20 A solução deve correlacionar os eventos de detecção e bloqueio de malwares, permitindo a visualização de relatório com todas as fases do ataque.

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 Ibama 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 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 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 Os agentes da solução deve ser compatível com as versões de Sistema Operacionais:

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

I - Microsoft Windows 7 (32-64bit) e superior em todas as suas distribuições(home, starter, professional, ultimate e enterprise).

6.4.1.2 Para servidores de rede físicos ou virtuais:

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

II - Ser suportado em sistemas operacionais linux, tais como Ubuntu, CentOS, Debian, Oracle Linux , Red Hat Enterprise, SUSE Linux Enterprise (32-64bit).

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

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

6.4.3 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.

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

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

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

6.4.7 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;

6.4.8 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 de um componente on-premises, para que tais equipamentos possam ser gerenciados, atualizados e protegidos.

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

6.5.2 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.

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

6.5.4 Permitir no mínimo 5(cinco) acessos simultâneos.

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

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

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

6.5.8 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.

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

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

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

6.5.12 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.

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

6.5.14 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.

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

6.5.15.1 Eventos de ameaças;

6.5.15.2 Eventos de comportamentos suspeitos;

6.5.15.3 Malwares detectados e bloqueados;

6.5.15.4 Computadores infectados.

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

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

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

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

6.5.19.1 Nome da máquina;

6.5.19.2 Endereço IP;

6.5.19.3 Versão do sistema operacional (incluindo a versão do Service Pack);

6.5.19.4 Versão do agente;

6.5.19.5 Política aplicada.

6.5.20 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.

6.6 Monitoramento Assistido:

6.6.1 Este serviço tem por objetivo operacionalizar as atividades de monitoração, detecção e resposta a incidentes de segurança, tratando os incidentes de forma coordenada, organizada e eficaz conforme necessidade do Ibama.

6.6.2 Deverá ser realizado de forma remota, externamente à CONTRATANTE, em dependências sob responsabilidade da CONTRATADA;

6.6.3 Deverá atuar na resposta à incidentes e ser realizado em língua portuguesa com monitoração em regime 12x5 (doze horas e cinco dias por semana);

6.6.4 Este serviço deverá ser prestado por equipe própria da CONTRATADA;

6.6.5 Este serviço deverá interagir com o CONTRATANTE via sistema de gestão e orquestração de incidentes de segurança da informação, sistemas disponibilizados pelo CONTRATANTE, ligação telefônica e correio eletrônico;

6.6.6 As solicitações e respostas de informações adicionais sobre os incidentes, como logs e evidências, devem ser anexadas ao tíquete registrado na ferramenta;

6.6.7 A CONTRATADA deverá garantir a prestação de serviço com disponibilidade mensal de 97% no regime de monitoração 12x5(doze horas e cinco dias por semana). Em casos de indisponibilidade, esta não deverá atingir períodos superiores a 4 horas consecutivas;

6.6.8 A CONTRATADA deverá apresentar plano de continuidade para a prestação deste serviço; Será considerado incidente de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do CONTRATANTE;

6.6.9 O serviço deverá atender os seguintes requisitos:

6.6.9.1 Monitorar ferramentas de segurança;

6.6.9.2 Monitorar o armazenamento dos logs de eventos e e incidentes de segurança;

6.6.9.3 Monitorar sistema de gestão, orquestração e automação de incidentes de segurança da informação, controlando eventos, alertas, painéis e incidentes;

6.6.9.4 Iniciar tratamento de incidentes em até 10 min;

6.6.9.5 Realizar triagem, classificação e categorização de eventos de segurança da informação;

6.6.9.6 Realizar triagem, classificação e categorização de incidentes de segurança da informação, também identificando casos de falso positivo;

6.6.9.7 Identificar incidentes de segurança da informação; Registrar, escalar e notificar incidentes de segurança da informação;

6.6.9.8 Registrar, escalar e notificar incidentes de segurança da informação;

6.6.9.9 Realizar coleta de dados, informações e evidências para inclusão no registro do evento ou incidente;

6.6.9.10 Executar ações de mitigação, contenção, diagnóstico, resolução e outros procedimentos necessários para tratamento de incidentes de segurança da informação, solicitados pelo CONTRATANTE;

6.6.10 Interagir com a ETIR e demais equipes da CONTRATANTE, podendo realizar ações em conjunto;

6.6.11 Registrar e documentar ações e procedimentos realizados;

6.6.12 Emitir relatório semanal estatístico das operações realizadas;

6.6.13 Emitir relatórios conforme necessidade, periodicidade e padrões estabelecidos pela CONTRATANTE;

6.6.14 Apoiar na definição, documentação e manutenção de Política de Gerenciamento de Eventos, contendo diretrizes para geração, coleta, retenção e classificação de eventos e monitoramento de logs;

6.6.15 Apoiar na definição, documentação e manutenção de estratégia de visibilidade de ameaças, devendo abordar: rotinas, periodicidade, métodos para identificação de novos casos de uso, utilização de fontes de visibilidade e inteligência de ameaças;

6.6.16 Apoiar na definição, documentação e manutenção da normas, diretrizes e Política de Segurança da Informação e Comunicação da CONTRATANTE , visando refletir as definições instituídas por esses serviços de monitoramento;

6.6.17 Apoiar na Análise de Requisitos Regulatórios, Contratuais e Legais que se referem à segurança da informação e aplicáveis a CONTRATANTE;

6.6.18 Apoiar na avaliação de Helth Check das soluções de segurança do CONTRATANTE, validando o mesmo e apresentando recomendações;

6.6.19 Apoiar na definição de ajustes e configuração de ferramentas de Segurança, apresentando recomendações a serem realizadas pela equipe técnica da CONTRATANTE.

6.6.20 Apoiar na realização de Avaliação da Utilização de ferramentas de Segurança, observando: regras, alertas, painéis, fontes de dados, automatizações, integrações, relatórios e dimensionamento; apresentar recomendações e indicações de melhores práticas no que se refere à monitoração, análises, casos de uso de forma eficiente; e participar da implementação das recomendações quando necessário;

6.6.21 Realizar Avaliação de Performance, com base nas métricas e indicadores definidos;

6.6.22 Gerar subsídios e recomendações para elaboração de conteúdos para divulgação de definições e orientações de segurança da informação e cibernética, a serem utilizados em ações de cultura e conscientização;

6.6.23 Apoiar na definição, documentação e manutenção de linha base (baseline) de comportamento para monitoração do ambiente de TI da CONTRATANTE, ajustando métricas e limiares de detecção, com o objetivo de reduzir o número de falsos positivos e aumentar a precisão da detecção;

6.6.24 Interagir com o sistema do CONTRATANTE para o processo de Gestão de Mudanças, Gestão de Incidentes de TI Gestão de requisições.

6.7 **Instalação da solução e repasse de conhecimento**

6.7.1 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 Ibama em Brasília, em dias úteis, no período de 8h00 às 12h00 e de 14h00 às 18h00.

6.7.2 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.

6.7.3 A disponibilização da solução de gerência e a instalação e configuração dos agentes da solução deverá ser concluída em 30 (trinta) dias corridos para a sede do Ibama e em até 60 (sessenta) dias corridos para as unidades nas demais localidades, contados a partir da assinatura da Ordem de Serviço, conforme item 6.7.4.

6.7.4 **A instalação compreenderá:**

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

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

6.7.4.3 Configuração de dashboards, relatórios e alertas, de maneira coordenada com o Ibama.

6.7.4.4 Customização dos pacotes de instalação dos agentes e distribuição a todas as estações do Ibama, inclusive nas unidades descentralizadas nos estados da federação.

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

6.7.4.6 Documentação da topologia da solução, relatório das atividades e configurações realizadas.

6.7.4.7 Apresentação da solução configurada e implantada.

6.7.4.8 Deverá ser realizado repasse de conhecimento da solução de gerência para 1 grupos de até 4 pessoas, oferecido por técnico certificado na solução.

6.7.4.9 No repasse de conhecimento deve ser utilizado material em português.

6.7.4.10 Não é necessário que o repasse seja feito para um grupo fechado do Ibama e o mesmo pode ser realizado de forma remota.

6.7.4.11 O repasse de conhecimento 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.

6.7.4.12 As datas dos repasses de conhecimento devem ser previamente combinadas com o Ibama.

6.7.4.13 Todas as despesas do repasse de conhecimento devem correr por conta da Contratada.

6.7.4.14 Caso o repasse de conhecimento seja ministrado presencialmente e fora de Brasília, deverão estar incluídas as despesas com passagens aéreas, hospedagem e traslado entre aeroporto, hotel e local de treinamento.

6.7.4.15 O Ibama se reserva o direito de solicitar novo repasse caso aquele oferecido venha a ser questionado com relação à qualidade ou à carga horária. Neste caso, eventuais despesas de locomoção e estadia serão ressarcidas ao Ibama pela Contratada.

6.7.4.16 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 repasse.

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

6.8 **Garantia**

6.8.1 A Contratada deverá fornecer garantia da solução pelo prazo de 12 (doze) meses, contados a partir da data da emissão do Termo de Recebimento, não se limitando ao término da vigência contratual.

6.8.2 Deverá ser oferecido suporte da Contratada, com possibilidade de abertura de chamados em regime de 12x5, de 8h00 às 20h00, nos dias comerciais, para resolução de problemas.

6.8.3 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.

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

6.8.5 A garantia deverá prover, obrigatoriamente:

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

6.8.5.2 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;

6.8.5.3 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;

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

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

6.8.6.1 No caso de manutenções preventivas, o horário do atendimento deverá ser compreendido entre 9h00 e 18h00, em dias úteis (5 x 9h);

6.8.6.2 No caso de manutenções corretivas, o horário do atendimento deverá ser compreendido entre 8h00 e 20h00, em dias úteis (5 x 12h);

6.8.6.3 O início do atendimento não poderá ultrapassar:

> I - O prazo de 2(duas) horas, contadas a partir da solicitação feita pelo Ibama, 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 Ibama, 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 Ibama, 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.).

6.8.6.4 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 Ibama, 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 48 (quarenta e oito) horas, contadas a partir da solicitação feita pelo Ibama, 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 72 (setenta e duas) horas, contadas a partir da solicitação feita pelo Ibama, 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.).

IV - Os prazos serão contados conforme previsto no item 6.9.

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

6.9 **Prazos para entrega e instalação da solução**

6.9.1 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.

6.9.2 A solução deverá estar completamente disponibilizada, instalada, configurada e operacional em até no máximo 60(sessenta) dias para a sede e 90 (noventa) dias corridos para as demais localidades do Ibama, contados a partir da data de assinatura da ordem de serviço. A implantação deve ocorrer em 3(três) etapas com o seguinte cronograma de implantação:

6.9.2.1 Para a sede do Ibama o prazo é de 60 (sessenta) dias corridos.

6.9.2.2 Para as localidades do Sul, Sudeste e Centro-Oeste do Ibama 90 (noventa) dias corridos.

6.9.2.3 Para as localidades do Norte e Nordeste do Ibama 90 (noventa) dias corridos.

6.9.3 A garantia deve ser imediata, contada a partir da data de emissão do Termo de Recebimento, pelo período total de 12 (doze) meses.

6.9.4 A entrega deve conter a garantia para 12 meses, e a cada aditivo contratual efetivado, deverá ser entregue nova garantia de mais 12 meses, e assim por diante, nos aditivos subsequentes.

6.9.5 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.

6.9.6 Os produtos componentes da solução devem ser oferecidos em sua última versão.

6.10 **Local de entrega e Instalação**

6.10.1 A solução deverá ser entregue no Edifício Sede do Ibama, em Brasília-DF, no seguinte endereço: SCEN Trecho 2 - Edifício Sede - L4 Norte - Brasília/DF - CEP: 70818-900.

6.10.2 A instalação da solução deverá ser realizada na Sede do Ibama e suas unidades descentralizadas. A distribuição e instalação dos agentes para as unidades descentralizadas do Ibama poderá ser realizada remotamente a partir da Sede.

6.11 **Da avaliação do nível mínimo de serviço (ANMS)**

6.11.1 Os níveis mínimos de serviços para as ordens de serviços serão apurados conforme o indicador abaixo:

IAE – INDICADOR DE ATRASO DE ENTREGA DE OS		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos produtos e serviços constantes na Ordem de Serviço.	
Meta a cumprir	IAE < = 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Ordens de Serviço dentro do prazo previsto.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de demandas, por controle próprio da Contratante e lista de Termos de Recebimento Provisório e Definitivo emitidos.	
Forma de acompanhamento	A avaliação será feita conforme linha de base do cronograma registrada na OS. Será subtraída a data de entrega dos produtos da OS (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da OS.	
Periodicidade	Mensalmente, para cada Ordem de Serviço encerrada e com Termo de Recebimento Definitivo.	
Mecanismo de Cálculo (métrica)	IAE = TEX – TEST TEST Onde: IAE – Indicador de Atraso de Entrega da OS; TEX – Tempo de Execução – corresponde ao período de execução da OS, da sua data de início até a data de entrega dos produtos da OS. A data de início será aquela constante na OS; caso não esteja explícita, será o primeiro dia útil após a emissão da OS. A data de entrega da OS deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da OS continua a correr, findando-se apenas quanto a Contratada entrega os produtos da OS e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da OS – constante na OS, conforme estipulado no Termo de Referência.	

Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para as OS de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante.
Início de Vigência	A partir da emissão da OS.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: De 0 a 0,10 – Pagamento integral da OS; De 0,11 a 0,20 – Glosa de 1% sobre o valor da OS; De 0,21 a 0,30 – Glosa de 5% sobre o valor da OS; De 0,31 a 0,50 – Glosa de 10% sobre o valor da OS; De 0,51 a 1,00 – Glosa de 15% sobre o valor da OS; Acima de 1 – Será aplicada Glosa de 20% sobre o valor da OS e multa de 5% sobre o valor do Contrato.

6.11.2 Os níveis mínimos de serviços para as chamados de atendimento de suporte corretivo deverão ser atendidos conforme a tabela abaixo:

Severidade	**Indicador**	**Prazo de 1º Atendimento**	**Solução Definitiva**
Alta	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.	02 (duas) hora	24 (vinte e quatro) horas.
Média	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.	04 (quatro) horas	48 (quarenta e oito) horas.
Baixa	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.	08 (oito) horas	72 (setenta e duas) horas.

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

6.11.2.2 Os níveis mínimos de serviços para as chamados de atendimento de suporte corretivo serão apurados conforme a tabela abaixo que aplica-se tanto para o prazo de 1º atendimento quanto para o prazo para a solução definitiva:

IAE – INDICADOR DE ATRASO PARA CORREÇÃO DE PROBLEMA		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso nos chamados para a correção de problemas. Aplica-se ao tempo de início de atendimento e o tempo total da correção do problema.	
Meta a cumprir	IAE <= 0	A meta definida visa garantir a resolução dos chamados dentro do prazo previsto e de acordo com a severidade.
Instrumento de medição	Através das ferramentas disponíveis para a gestão de chamados, por controle próprio da Contratante e lista de Termos de Recebimento Provisório e Definitivo emitidos.	
Forma de acompanhamento	A avaliação será feita conforme os dados de abertura de chamados.	
Periodicidade	Mensalmente, para cada chamado realizado.	
Mecanismo de Cálculo (métrica)	IAE = TEX – TEST TEST Onde: IAE – Indicador de Atraso de Chamado; TEX – Tempo de Execução – corresponde ao período de início de atendimento ou de solução do chamado, da sua data/hora de início até a data/hora de início de atendimento/solução do chamado. A data/hora de início será a da abertura do chamado; A data de início de atendimento/solução do chamado deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes no Termo de Referência. Para os casos em que o fiscal técnico rejeita a data de início de atendimento/solução, o prazo de execução do chamado continua a correr, findando-se apenas quanto a Contratada realizar o início de atendimento/concluir a solução do chamado e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para o início/solução do chamado – constante no registro de chamado, conforme estipulado no Termo de Referência.	
	Obs1: Serão utilizados horas de acordo com os requisitos do item 4.4.6 na medição.	

Observações	Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como horas úteis no cômputo do indicador. Obs3: Não se aplicará este indicador para chamados de Manutenções Corretivas do tipo Garantia e aquelas com execução interrompida ou cancelada por solicitação da Contratante.
Início de Vigência	A partir da abertura do chamado.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: De 0 a 0,10 – não se aplicam glosas; De 0,11 a 0,20 – Glosa de 0,1% sobre o valor do serviço mensal do item 4; De 0,21 a 0,30 – Glosa de 0,5% sobre o valor do serviço mensal do item 4; De 0,31 a 0,50 – Glosa de 1,0% sobre o valor do serviço mensal do item 4; De 0,51 a 1,00 – Glosa de 5,00% sobre o valor do serviço mensal do item 4; Acima de 1 – Será aplicada Glosa de 10% sobre o valor mensal do item 4.

6.12 **Do pagamento mensal dos serviços de monitoramento**

6.12.1 O serviço mensal será mensurado por meio de diversos elementos, decorrente da formação de preços, que produzirá um Valor Mensal do Serviço - VMS, que será determinado pela seguinte fórmula:

Serviços de monitoramento:
VMS = [VS] - [FR]

Onde:

- [VS]: Valor Mensal do serviço de monitoramento.
- [FR]: Fator de Redução (glosa) - Os serviços serão avaliados mensalmente e caso exista desvio na avaliação mensal dos serviços, a fórmula de cálculo terá Fator de Redução.

6.13 **Do pagamento único das licenças por contrato firmado**

6.13.1 As licenças serão pagas de acordo com o quantitativo que constará no contrato e na ordem de serviço que produzirá um Valor Único de Licenças - VUL, que será determinado pela seguinte fórmula:
VUL = ([QLD] * PUD + [QLS] * [PUS]) - [FR]

- QLD: Quantidade de licenças unidades contratadas para os desktops/notebooks.
- QLS: Quantidade de licenças de servidores contratadas.
- PUD: Preço unitário de licenças contratadas para os desktops/notebooks.
- PUS: Preço unitário de licenças contratadas para os servidores.
- FR: Fator de Redução (glosa) - Os serviços serão avaliados quanto ao prazo de entrega e instalação e caso exista desvio na avaliação, a fórmula de cálculo terá Fator de Redução.

6.14 **Do pagamento anual da atualização das licenças e garantia por 12 meses**

6.14.1 O valor anual do serviço de atualização será remunerado anualmente no aniversário do contrato e serão pagas de acordo com o quantitativo que constará no contrato e na ordem de serviço que produzirá um Valor Anual de Atualização - VAA, que será determinado pela seguinte fórmula:
VAA = ([QLD] * PAD + [QLS] * [PAS]) - [FR]

- QLD: Quantidade de licenças unidades contratadas para os desktops/notebooks.
- QLS: Quantidade de licenças de servidores contratadas.
- PAD: Preço unitário do valor anual(por 12 meses) da atualização das licenças contratadas para os desktops/notebooks.
- PAS: Preço unitário do valor anual(por 12 meses) da atualização das licenças contratadas para os servidores.

7. Estimativa das Quantidades a serem Contratadas

7.1 **Estimativa da demanda**

7.1.1 A estimativa total de equipamentos a serem protegidos e os serviços a serem contratados é o que consta na tabela abaixo:

ITEM	DESCRIÇÃO	UND.	QTDE
1	Serviço de proteção para computadores e notebooks	UNIDADE	4900
2	Serviço de proteção para servidores de rede		180
3	Serviço de monitoramento assistido	MENSAL	12

7.1.3 O quantitativo foi estimado/definido com base no seguinte critério, que reflete a quantidade computadores, notebooks e servidores em uso no Ibama.

Item de Configuração	Parque Ibama
Computador desktop	4116
Computador Notebook	771
Margem de segurança com 13 unidades	13
Total estimado	**4900**

Referência: SEI 10536113.

Item de Configuração	Parque Ibama
Servidores virtuais Ibama	144
Margem de segurança com 36 unidades ou 25%	36
Total estimado	**180**

Referência: SEI 10365041.

7.1.4 Este item é apenas de estimativa de demanda, a disposição final dos itens será definido no estudo de solução viáveis e na escolha da solução mais viável para a contratação.

8. Estimativa do Valor da Contratação

8.1 **Análise de soluções**

Serão analisadas as opções disponíveis para o provimento da solução de proteção objeto deste estudo.

8.1.1 **Identificação das possíveis soluções:**

Solução	**Descrição**
Solução 1	Aquisição de licenças e contratação do Serviços de Monitoramento Assistido por 12 meses + projeção de 30% de custo de atualização em nova contratação por 12 meses e renováveis até o limite de 60 meses.
Solução 2	Contratação de subscrição de licenças On-Premisse e Serviços de Monitoramento Assistido por 12 meses renováveis até o limite de 60 meses.
Solução 3	Contratação de Subscrição de licenças em nuvem e Serviços de Monitoramento Assistido por 12 meses renováveis até o limite de 60 meses.
Solução 4	Aquisição de licenças com atualização garantida por 60 meses e contratação do Serviços de Monitoramento Assistido por 12 meses renováveis até o limite de 60 meses.
Solução 5	Aquisição de licenças com atualização garantida por 12 meses, contratação de serviço de atualização por 12 meses a partir do segundo ano até o limite de 48 meses e contratação do Serviços de Monitoramento Assistido por 12 meses até o limite de 60 meses.

8.1.2 **Análise comparativa das soluções**

Requisito	**Solução**	**Sim**	**Não**	**Não se Aplica**
Requer infraestrutura de TI no Ibama	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
	Solução 4	X		
	Solução 5	X		
Requer a instalação de Clientes em máquinas de usuários e servidores de rede	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
	Solução 4	X		
	Solução 5	X		
Podem ter o volume ajustado a demanda do Ibama e acrescentar e reduzir o número de licenças	Solução 1		X	
	Solução 2	X		

	Solução 3	X		
	Solução 4		X	
	Solução 5		X	

8.1.3 **Registro de soluções consideradas inviáveis**

Dentre as soluções 1 a 5 , não há registro, do ponto de vista técnico, de solução inviável nesta análise, desta forma a análise ser mediante o custo total de propriedade.

8.1.4 Análise comparativa de Custos (TCO)

Cálculo dos custos totais de propriedade

- Mapa comparativo dos cálculos totais de propriedade (TCO)

Cenário	DESCRIÇÃO	ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	Total em 5 anos
1	Aquisição de licenças e contratação do Serviços de Monitoramento Assistido	1.510.204,15	705.061,25	705.061,25	705.061,25	705.061,25	4.330.449,13
2	Subscrição de licenças On-Premisse e Serviços de Monitoramento Assistido	1.258.398,00	1.258.398,00	1.258.398,00	1.258.398,00	1.258.398,00	6.291.990,00
3	Subscrição de Licenças em nuvem e Serviços de Monitoramento Assistido	887.357,47	887.357,47	887.357,47	887.357,47	887.357,47	4.436.787,33
4	Aquisição de Licenças e atualização por 60 meses	3.626.074,80	360.000,00	360.000,00	360.000,00	360.000,00	5.066.074,80
5	Aquisição de licenças e pagamento anual da atualização	1.664.452,20	553.022,80	553.022,80	553.022,80	553.022,80	3.876.543,40

- Descrição da solução de tecnologia da Informação a ser contratada
  - A solução mais viável do ponto de vista das necessidades dos gestores do Ibama é a solução 5, que adquire as licenças uma única vez, contrata o serviço de atualização a partir do segundo ano até o limite de 48 meses e contrata o serviço de monitoramento por 12 meses até o limite de 60 meses.
- Estimativa de custo total da contratação
  - A estimativa total de despesa com a contratação ao longo de 5 anos é de R$ 3.876.543,40 (3 milhões, oitocentos e setenta e seis mil, quinhentos e quarenta e três reais e quarenta centavos).
  - A estimativa para os primeiros 12(doze) meses é de um desembolso de R$ 1.664.452,20 (hum milhão, seiscentos e sessenta e quatro reais, quatrocentos e cinquenta e dois reais e vinte centavos).
  - A estimativa de desembolso do segundo ao terceiro ano é de R$ 553.022,80 (Quinhentos e cinquenta e três mil, vinte e dois reais e oitenta centavos).

- Os valores e a planilha de projeção estão descritas no processo na nota técnica de pesquisa de preços e na planilha auxiliar de memória de cálculo. Para esta análise, quando em estrutura local, foi projetado o valor deste custo, de modo que fosse possível aproximar a comparação ao máximo possível, haja vista que em nuvem todos os custos estão embutidos nos serviços.

O valor final da contratação segue apresentado abaixo e não considera os custos de infraestrutura para a sustentação dos serviços, haja vista que a contratação trata-se apenas de itens de NGAV e a infraestrutura será inicialmente a disponível no Ibama, que em um futuro breve pode ser movida para um serviço em nuvem, cujo custeio será do Ibama.

GRUPO /ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO ESTIMADO (R$)	VALOR TOTAL ESTIMADO (R$)
1	Aquisição/Contratação de solução de proteção para computadores desktops e notebooks com suporte e garantia por 12 meses.	Unidade	4900	140,72	689.528,00
2	Aquisição/Contratação solução de proteção para servidores de rede com suporte e garantia por 12 meses.	Unidade	180	343,90	61.901,40
3	Serviço de garantia, suporte e atualização por 12 meses para o item 1, a partir do segundo ano de contrato	Anual	1	166.941,00	166.941,00
4	Serviço de garantia, suporte e atualização por 12 meses para o item 2, a partir do segundo ano de contrato	Anual	1	26.081,80	26.081,80
5	Serviço de monitoramento assistido	Mensal	12	14.166,67	170.000,04
VALOR TOTAL DA ESTIMATIVA					1.114.452,24

Esses valores constam no informado no documento SEI 10530917 e 10535198.

9. Justificativa para o Parcelamento ou não da Solução

9.1 **Justificativa para o não parcelamento do objeto**

9.1 Não será adotado para esta licitação o parcelamento dos itens. Desta forma, os itens serão licitados em um só lote/grupo, pois há uma interdependência entre eles e também por se tratar de uma solução de segurança que se complementam e necessitam de profissionais especialistas providos por um único fabricante. Essa estratégia procura maximizar a efetividade da proteção da rede

do Ibama e possibilitar a atribuição da responsabilidade a apenas um fornecedor sem conflito de competências e especialidades. Não por exemplo como separa o serviço de monitoramento assistido da licença, pois não seria possível associar o serviço sem saber que fabricante será o fornecedor da licença.

10. Contratações Correlatas e/ou Interdependentes

10.1 **Contratações Correlatas ou Interdependentes**

10.1 Não há necessidade de contratação correlatas ou interdependentes, haja vista que os desktops, notebooks e servidores a serem protegidos já estão instalados no Ibama.

11. Alinhamento entre a Contratação e o Planejamento

11.1 **Alinhamento estratégico da contratação**

11.1.1 A contratação está alinhada com o PDTIC 2020-2023-v3, conforme abaixo:

ALINHAMENTO AO PDTIC -2020-2023-v3			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
A6.1	Contratar e manter serviços de suporte, monitoramento e respostas a incidentes de Segurança da Informação para usuários	N6.1	Solução de segurança para usuários
A6.2	Contratar e manter serviços de suporte, monitoramento e respostas a incidentes de Segurança da Informação para datacenter	N6.2	Solução de segurança para o datacenter

11.1.2 O Alinhamento com o Plano Anual de Contratação está informado abaixo:

ALINHAMENTO AO PAC 2020	
1000	Software

11.1.3 Haja vista que o Plano Anual de Contratação - PAC para essa demanda foi realizado com um ano de antecedência, o escopo deste estudo foi ampliado em decorrência da necessidade de maior detalhamento, assim, o escopo de itens desta contratação contém mais itens quando comparado com o que foi planejado.

12. Resultados Pretendidos

12.1 **Os resultados a serem alcançados são:**

- Minimizar o máximo possível incidentes de seguranças que envolvam a rede do Ibama
- Permitir a atualização concorrente dos sistemas operacionais
- Elevar o nível de proteção dos computadores desktops e notebooks do Ibama

- Elevar o nível de proteção dos servidores em operação no Ibama

13. Providências a serem Adotadas

13. **Providências adicionais**

13.1 Nenhum providência adicional ou ajuste para a utilização da solução de proteção contratada será necessária.

14. Possíveis Impactos Ambientais

14. **Análise de possíveis impactos ambientais**

14.1 Como se trata puramente de licença de software e de serviços não vislumbra-se impactos ambientais com a utilização desta solução de proteção.

15. Declaração de Viabilidade

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

15.1. 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 Ibama, portanto, o presente Estudo Técnico Preliminar é justificadamente viável quanto aos requisitos de negócios, administrativos e técnicos a serem alcançados.

16. Responsáveis

Em atendimento ao art. 11, Inciso V, § 1º e 3º, da Instrução Normativa/SGD/ME nº 01/2019, como integrante técnico, aprovo o presente Estudo Técnico Preliminar.

CLEITON ARAUJO DE OLIVEIRA

Integrate Técnico

Em atendimento ao art. 11, Inciso V, § 1º e 3º, da Instrução Normativa/SGD/ME nº 01/2019, como integrante requisitante, aprovo o presente Estudo Técnico Preliminar.

MOSAR RODRIGUES RABELO JUNIOR

Integrante Requisitante