ESTUDO TÉCNICO PRELIMINAR

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. Este Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da necessidade identificada e registrada no Documento de Oficialização da Demanda (110770174), bem como demonstrar a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, em consonância com a Lei 14.133/2021, Decreto Estadual 48.816/2023, e os demais normativos vigentes.

1.2. A demanda surgiu a partir da necessidade identificada por meio do despacho (110420825), no qual a Diretoria de Infraestrutura Tecnológica, solicita a contratação de uma Solução de Gerenciamento Unificado de ativos em nuvem.

1.3. A iniciativa surge da necessidade de aprimorar o controle sobre os acessos e o uso dos recursos tecnológicos da organização, assegurando maior visibilidade sobre as interações realizadas e promovendo a consistência, a disponibilidade e a confiabilidade dos serviços prestados.

1.4. O PRODERJ, instituição vinculada à Secretaria de Estado de Transformação Digital, atua como Órgão Gestor da Tecnologia da Informação, sendo responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, as bases de dados de vários órgãos estaduais e os diversos equipamentos hospedados no Data Center do Estado.

1.5. A tarefa de manter a área de TI sempre alinhada ao planejamento estratégico do PRODERJ constitui-se um desafio permanente. Busca-se garantir em todas as questões relacionadas à infraestrutura de TI, que o foco se mantenha na estratégia e nas necessidades da Autarquia. Além desta, existe também a tarefa e obrigação de manter o ambiente tecnológico íntegro, confiável e de preservar a qualidade dos serviços por ele providos sempre alinhados.

1.6. O presente estudo reúne as justificativas técnicas para o atendimento da demanda, a análise comparativa de soluções tecnológicas possíveis e, por fim, a recomendação da alternativa que melhor equilibra custo, efetividade, viabilidade de implantação e aderência aos normativos de segurança e proteção de dados. Com isso, busca-se garantir que qualquer eventual contratação futura esteja devidamente fundamentada em critérios técnicos, em conformidade com os princípios da economicidade, eficiência e legalidade.

1.7. Este documento tem como objetivo apresentar os desafios enfrentados pela organização em relação à gestão de ativos de tecnologia da informação, destacando os impactos da ausência de controle eficaz sobre esses recursos. Atualmente, o PRODERJ enfrenta obstáculos significativos relacionados à visibilidade e ao controle dos ativos em uso, sejam eles físicos, virtuais ou lógicos e na a proteção de arquivos pessoais e dados armazenados nesses ativos. A inexistência de um inventário unificado, confiável e atualizado compromete o planejamento estratégico de TI e dificulta a gestão eficiente dos recursos, resultando em situações como aquisição redundante de licenças, manutenção de ativos obsoletos ou subutilizados, e desafios no processo de desativação de recursos que já não são mais utilizados.

1.8. Além disso, a falta de visibilidade sobre os ativos compromete significativamente a capacidade de manter um ambiente tecnológico seguro e controlado. Dispositivos não monitorados, sistemas desatualizados e softwares não autorizados podem originar falhas que afetam a estabilidade e a confiabilidade da infraestrutura de TI. Esse cenário impacta a integridade dos dados e dos serviços essenciais da organização, podendo resultar em interrupções operacionais, exposição indevida de informações sensíveis e danos à imagem institucional.

1.9. Destaca-se ainda a crescente dificuldade em atender auditorias internas e externas. Sem dados consolidados e evidências automatizadas de controle sobre ativos e segurança, a área de TI é forçada a recorrer a processos manuais, suscetíveis a erros e inconsistências, o que compromete a credibilidade das informações apresentadas e o cumprimento dos prazos exigidos por auditores e órgãos reguladores.

1.10. Atualmente o PRODERJ não possui solução centralizada e automatizada para realizar o inventário e a gestão dos ativos de tecnologia da informação. O controle dos ativos é feito de forma descentralizada, por meio de processos manuais ou planilhas que não garantem precisão, atualidade ou padronização dos dados.

1.11. Essa limitação compromete diretamente a eficiência operacional da infraestrutura de TI, pois não há:

- Visibilidade consolidada sobre os equipamentos e softwares utilizados.
- Mecanismos para identificar obsolescência, subutilização ou redundância de ativos.
- Capacidade técnica de responder rapidamente a demandas de manutenção ou expansão.
- Controle efetivo sobre licenciamento, versionamento e compatibilidade de softwares.
- Apoio técnico automatizado para processos de atualização, substituição ou descarte de equipamentos.

1.12. Diante das atribuições do PRODERJ na proteção e controle de sistemas, dados e ativos críticos, torna-se imprescindível que o órgão invista em uma solução de gerenciamento unificado de ativos junto a uma adoção de práticas e soluções alinhadas ao Decreto Estadual nº 48.891/2024.

1.13. O Decreto Estadual nº 48.8891/2024 estabelece diretrizes estratégicas e operacionais voltadas à governança da segurança da informação, incluindo o gerenciamento de ativos, controle de acessos, inventário de software, criptografia de dados, configuração segura, aplicação de correções, coleta de registros de auditoria, entre outros.

1.14. Vivemos um cenário onde a complexidade dos ambientes tecnológicos e a expansão constante de dispositivos conectados exigem dos gestores públicos maior controle e visibilidade sobre seus ativos. A ausência de ferramentas que ofereçam inventário unificado e monitoramento em tempo real dificulta a administração eficiente da infraestrutura, tornando essencial o investimento em soluções que fortaleçam a governança e o uso racional dos recursos tecnológicos.

1.15. A iniciativa contempla desde ações básicas, como o inventário e o controle de ativos, até níveis mais avançados de governança tecnológica, promovendo maior organização, padronização e rastreabilidade dos recursos de TI. Entre os principais benefícios, destacam-se:

- Visualização imediata e precisa de todos os ativos conectados à rede;
- Facilidade no planejamento de renovação do parque computacional;

- Garantia de aderência a contratos de licenciamento, evitando redundâncias;
- Identificação de máquinas com recursos insuficientes ou subutilizados;
- Apoio à tomada de decisões sobre aquisição, alocação e readequação de ativos;
- Automatização de processos, promovendo agilidade e redução de retrabalho.

1.16. Importa ressaltar que sem a garantia de visibilidade total dos ativos e softwares em uso, pode-se enfrentar falta de controle sobre dispositivos ou programas não autorizados e a proteção de dados e informações. Através da adoção de controles como o inventário detalhado de ativos, a utilização de ferramentas de descoberta ativa e passiva, o gerenciamento adequado de software autorizado, e a criptografia de dados sensíveis, o Decreto Estadual nº 48.891/2024 proporciona uma base sólida para a proteção da informação.

1.17. Outro aspecto essencial é a gestão de aplicação de patches. A não correção de falhas conhecidas é uma das principais causas de violações de dados. Diretrizes, como a execução automatizada de patches do sistema operacional e de aplicações, e a realização de varreduras automatizadas, são fundamentais para automatizar esse processo, evitando atrasos humanos e garantindo agilidade na resolução de problemas.

1.18. A utilização de ferramentas de gerenciamento automatizado de patches é indispensável para garantir a conformidade com as diretrizes, remediação contínua e aplicação automatizada de atualizações. Essas ferramentas reduzem o tempo de resposta, garantem a consistência dos ambientes, até mesmo em infraestruturas heterogêneas.

1.19. A inexistência de uma estratégia clara de continuidade operacional, compromete a capacidade da organização de reagir prontamente a falhas nos serviços ou interrupções inesperadas. A ausência de um processo estruturado que envolva mecanismos de registro, comunicação e análise dos eventos impacta diretamente a disponibilidade dos sistemas e a eficiência institucional.

1.20. Com a expansão do trabalho remoto, a superfície de ataque da organização cresceu exponencialmente. Isso significa que os endpoints passaram a operar em redes não confiáveis, fora da visibilidade direta da TI, o que dificulta a aplicação de políticas centralizadas de gerenciamento. Nesse cenário, torna-se fundamental adotar uma solução de Gerenciamento Unificado de Endpoints (UEM) que permita aplicar controles, políticas e monitoramento contínuo, independentemente da localização do dispositivo.

1.21. A ausência de uma base de dados precisa e atualizada dos ativos corporativos representa uma lacuna crítica na segurança da informação. A inexistência de visibilidade abrangente sobre os dispositivos conectados à rede limita a capacidade de gerenciamento da infraestrutura, dificultando a aplicação de atualizações, a verificação da integridade de sistemas e aplicações, bem como a identificação de equipamentos que não atendem aos padrões previamente estabelecidos. A implementação de soluções de discovery e inventário automatizado de ativos, integradas a bases CMDBs ou plataformas de ITAM (IT Asset Management), é essencial e sem isso, a gestão de ativos torna-se reativa, baseada em suposições e altamente propensa a falhas.

1.22. Dispositivos com configurações divergentes e não alinhadas a padrões de segurança corporativa representam potenciais de impacto significativos. A padronização de configurações seguras é essencial para mitigar ataques que exploram falhas de configuração. Ferramentas de gerenciamento de configuração e compliance permitem aplicar, auditar e corrigir desvios em larga escala.

1.23. Ambientes corporativos modernos são compostos por uma variedade de sistemas operacionais e dispositivos, exigindo soluções que ofereçam cobertura e gerenciamento unificado. A utilização de ferramentas fragmentadas para cada tipo de sistema reduz a eficiência operacional e abre brechas de segurança. A adoção de soluções integradas para o inventário e gestão de ativos, aplicação de políticas de configuração segura, controle de acesso e monitoramento centralizado é essencial para garantir uma administração coesa, uma política uniforme de segurança e visibilidade consolidada sobre todos os ativos da organização.

1.24. Usuários frequentemente instalam software não autorizado, conectam mídias removíveis ou alteram configurações de segurança sem o devido conhecimento técnico. Isso gera um ambiente propenso a erros e facilita ataques baseados em engenharia social ou malwares introduzidos por ações imprudentes. Conforme as diretrizes do Decreto Estadual nº 48.891/2024, é necessário adotar mecanismos que combinem controle de aplicações, listas de permissões de software autorizado, bloqueios automatizados, e restrições baseadas em políticas de segurança.

1.25. No que diz respeito ao gerenciamento de EndPoints, o Gartner define ferramentas de gerenciamento de EndPoints como plataformas que oferecem gerenciamento de configuração, aplicação de patches e implantação de sistemas operacionais e aplicativos para computadores ou dispositivos móveis. Essas ferramentas são essenciais para manter a higiene cibernética e permitir operações e automação de computação do usuário final, facilitando a implantação de sistemas operacionais e aplicativos, aplicação de patches e gerenciamento de configurações.

1.26. A detecção tardia de incidentes compromete diretamente a capacidade de conter ataques antes que causem danos significativos. É imprescindível contar com soluções capazes de reconhecer ações que não seguem os padrões operacionais definidos, isolar dispositivos afetados e iniciar ações corretivas automaticamente. A adoção de ferramentas que possibilitem a coleta e análise contínua de logs, identificação de padrões de uso incomuns. e resposta automatizada a incidentes é fundamental para garantir uma postura proativa e responsiva.

1.27. A gestão de EndPoints exige investimentos estratégicos em ferramentas, capacitação e automação. Tentativas de manter processos manuais ou ferramentas isoladas aumentam a carga operacional, comprometem a eficácia das medidas de segurança e elevam o custo total de propriedade (TCO) em longo prazo. A adoção de plataformas integradas de segurança e gerenciamento promove sinergia entre as áreas técnicas, otimiza recursos e reduz a sobrecarga das equipes de segurança.

1.28. Como forma de prevenção contra possíveis incidentes e com o objetivo de elevar os níveis de segurança dos serviços prestados pelo PRODERJ aos Órgãos da Administração Pública Estadual, protegendo a integridade e a confidencialidade das informações que transitam pela Rede Governo, é fundamental que o PRODERJ disponha uma solução de gerenciamento unificado de ativos baseada em nuvem. Essa solução deve permitir visibilidade contínua e controle centralizado. Tal iniciativa contribui para a robustez e a consistência do ambiente compartilhado, além de viabilizar futuras aquisições integradas por outros órgãos da Administração Estadual, promovendo padronização, otimização de recursos e escalabilidade.

1.29. A tarefa de manter a área de TI sempre alinhada ao planejamento estratégico do PRODERJ constitui-se desafio permanente. Busca-se garantir em todas as questões relacionadas à infraestrutura de TI, que o foco se mantenha na estratégia e nas necessidades fins da Autarquia. Além desta, existe também a tarefa e obrigação de manter o ambiente tecnológico íntegro, confiável e de preservar a qualidade dos serviços por ele providos sempre alinhados à estratégia do PRODERJ.

1.30. Para contribuir na manutenção dos níveis de serviço oferecidos pelo PRODERJ aos demais órgãos da Administração Pública, bem como se preparar para oferecer novos serviços na vanguarda da tecnologia da informação, é necessário ser capaz de fazer a adequada gestão do inventário de ativos de hardware e software.

1.31. Os principais benefícios desta contratação serão:

- Estabelecer controle centralizado sobre os ativos corporativos, permitindo visibilidade em tempo real dos dispositivos conectados à rede e seus respectivos estados de conformidade.
- Aprimorar a configuração e o gerenciamento dos dispositivos por meio da aplicação automatizada de políticas, remoção de softwares não autorizados e desativação de serviços em desuso, visando maior eficiência operacional e conformidade com os padrões estabelecidos.
- Mitigar a disseminação de códigos maliciosos, aplicando correções de segurança (patches) de forma contínua e gerenciando o inventário de software e hardware com precisão.

- Auxiliar na conformidade com normativas e boas práticas de segurança da informação, como as diretrizes do Programa de Privacidade e Segurança da Informação (PPSI), garantindo a rastreabilidade das ações executadas nos endpoints.
- Aumentar a eficiência operacional da área de TI, através da automação de tarefas de configuração, inventário, atualizações automatizadas, dashboards atualizados em tempo real.
- Aprimorar os processos já existentes de auditoria e investigação por meio da coleta estruturada de logs e eventos, permitindo a análise detalhada de atividades fora dos padrões estabelecidos.
- Reduzir o risco de perda de dados sensíveis, por meio de políticas de criptografia em dispositivos de usuário final e mídias removíveis.

1.32. Ademais, o objeto proposto na presente demanda contribuirá para o atendimento da Lei 13.709/2018, Lei Geral de Proteção a Dados (LGPD) que intensifica a obrigatoriedade de proteção e privacidade dos dados dos titulares, no nosso caso, os cidadãos, reforçando a necessidade do PRODERJ, Órgão de Tecnologia do Estado, contratar e fornecer aos demais Órgãos da Administração Pública, uma solução capaz de garantir a integridade e a continuidade dos ativos de TIC diante das diversas situações adversas que podem comprometer seu funcionamento., conforme observamos no Art. 46 da LGPD, onde consta: “Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.”

1.33. Diante do exposto, o presente estudo examinará a possibilidade do fornecimento de uma solução de gerenciamento unificado de ativos em nuvem.

2. RELATO DESCRITIVO ACERCA DE CONTRATAÇÕES ANTERIORES VOLTADAS AO ATENDIMENTO DE NECESSIDADE IDÊNTICA OU SEMELHANTE, CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES A ATUAL

2.1. Não há contratações correlatas ou interdependentes previstas, uma vez que o objeto em tela não compõe, no todo ou em parte, nenhum objeto de contrato ou outras soluções existentes na Autarquia.

3. INSTRUMENTO DE PLANEJAMENTO

3.1. A previsão desta contratação foi incluída no PCA – Plano de Contratações Anual desta autarquia conforme abaixo:

ID PCA no PNCP: 42498600000171-0-000041/2025

Data de publicação no PNCP: 01/08/2024

ID do item no PCA: 24635

3.2. Alinhamento Estratégico

3.2.1. A contratação deste objeto se encontra prevista no Plano Estratégico e Diretor de Tecnologia da Informação e Comunicação - PEDTIC (110771928) do PRODERJ:

- **Objetivo Estratégico 1** - Prover, manter e atualizar a infraestrutura e as Soluções e Serviços de Tecnologia da Informação e Comunicação: Prover continuamente a inovação tecnológica para compor e atualizar a infraestrutura, as Soluções e os Serviços de Tecnologia da Informação e Comunicação, atendendo às crescentes demandas da Autarquia e dos Órgãos do Poder Executivo Estadual, visando o desenvolvimento, manutenção, integração e a padronização da TIC do estado (Alinhamento ao PPA 2024-2027 - Programa: 0493 / Ações: 1293 e 1294);
- **Objetivo Estratégico 2** - Ampliar a capacitação técnica e profissional dos servidores em TIC: Promover a qualificação exponencial dos servidores por meio da capacitação e participação em eventos que desenvolvam e aprimorem suas competências e a gestão do conhecimento em TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1293);
- **Objetivo Estratégico 3** - Aprimorar os Processos de TIC: Promover a melhoria contínua dos processos, métodos e técnicas gerando uma maior efetividade na gestão e no uso dos recursos que fornecem as soluções de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1294);
- **Objetivo Estratégico 6** - Garantir os padrões de qualidade dos serviços e soluções de TIC: Assegurar que os serviços de TIC prestados pelo PRODERJ atendam seus requisitos mínimos, suprindo as expectativas dos órgãos da Administração Pública Direta e Indireta, de modo que contribuam para a agregação de seus valores institucionais e o cumprimento de seus objetivos estratégicos, potencializando sua capacidade de entrega, reforçando a aptidão em produzir, entregar novas soluções e aprimorar as existentes, assim como, o fornecimento de uma infraestrutura inovadora que garantam que os recursos tecnológicos investidos sejam capazes de preservar e promover a segurança, a privacidade, a disponibilidade e a continuidade dos serviços públicos, reduzindo os riscos inerentes aos serviços de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ações 1293 e 1294).

4. ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Necessidade: Solução de Gerenciamento Unificado de Ativos em nuvem

4.1.2. Funcionalidades:

- **Console/gerenciamento -** A plataforma deve possuir console web com acesso a todas as funcionalidades da solução, garantindo uma interface única para o gerenciamento dos endpoints.
- **Arquitetura** - A solução deve ser disponibilizada como uma oferta software como serviço "SaaS", capaz de gerenciar até 2000 ativos, sem necessidade de instalação de componentes no datacenter do cliente, VPN ou acesso via rede corporativa. Esta solução SaaS pronta para uso deve ser hospedada fisicamente no Brasil.
- **Inventário e Descoberta** - Oferecer funcionalidade de descoberta para identificar novos dispositivos não gerenciados que se conectam à rede e sem agente instalado.
- **Medição de Uso de Software** - Medir o uso de softwares instalados com métricas de tempo e frequência de uso para Windows e MacOS.
- **Empacotamento e Distribuição de Software -** Deve permitir que um grupo de softwares seja atualizado de forma dinâmica conforme novas versões das aplicações que o compõem sejam lançadas, facilitando a manutenção de versões atualizadas sem a necessidade de modificar manualmente o grupo de software.
- **Gerenciamento de Configurações Diversas** - A solução deve permitir upload, download e remoção de arquivos nos endpoints.

- **Patch Management** - Deve possuir repositório centralizado para download de patches disponibilizadas pelos fabricantes do sistema operacional sem a necessidade de empacotamento pelos administradores da solução.
- **Relatórios** - Deve disponibilizar relatórios pré-definidos com os principais usos da ferramenta, permitindo cloná-los para customização.
- **Pontuações de Risco -** A solução deve calcular uma pontuação de risco de todo o ambiente de ativos com apresentação da evolução dessa pontuação ao longo do tempo.
- **Certificados Digitais -** Deve ser possível visualizar os certificados digitais utilizados no ambiente em dispositivos, permitindo a identificação rápida de: Certificados digitais expirados ou perto da data de expiração.
- **Experiência do Usuário** - Permitir customizar, agendar e definir público-alvo de surveys, com oferta direta na área de trabalho do usuário, sem a necessidade de componentes e integrações adicionais, facilitando a captura da "voz do cliente " em relação aos serviços de TI ofertados para Windows e MacOS.
- **Desempenho** - Possuir capacidade para cálculo automático de "Scores" para mensuração de experiência do funcionário com base nos dados obtidos do endpoint para Windows, Linux e MacOS.
- **Agente** - A solução deve executar todos os requisitos usando um único agente unificado.
- **Enforcement** - Configurações de Segurança - A solução deve realizar o gerenciamento de configurações de segurança, que incluir a capacidade de aplicar e gerenciar configurações de segurança de forma centralizada, garantindo que as políticas de segurança sejam aplicadas de forma consistente em todos os endpoints.
- **Detecção proativa** - A solução deve possuir recurso para automação de respostas de segurança, permitindo a configuração de respostas automáticas a eventos detectados.
- **Monitoramento de integridade e dados confidenciais** – A solução deve realizar o monitoramento contínuo de arquivos, diretórios e chaves de registro.
- **Automação** - A solução deve incluir recursos de automação sem código que permitem a configuração de múltiplas ações em sequência, incluindo controles e notificações na sequência de automação.

4.1.3. As demais especificações estão descritas no ANEXO I deste documento.

4.2. **Requisitos de Capacitação**

4.2.1. A CONTRATADA deverá prestar a devida capacitação, de forma on-line, aos usuários (servidores, técnicos e gestores) indicados pela CONTRATANTE, no formato workshop prático (hands on) ou online, de forma a preparar os usuários para a operacionalização do sistema.

4.2.2. O treinamento deverá abordar no mínimo: o uso da ferramenta, instalação, configuração, operação da ferramenta, gerenciamento, resolução de problemas.

4.2.3. A CONTRATADA deverá fornecer apostilas e vídeoaula contendo o material necessário a capacitação ofertada;

4.2.4. As capacitações poderão ser solicitadas a qualquer tempo para a CONTRATADA sem custos adicionais ao CONTRATANTE, durante todo o período de contrato;

4.2.5. O fornecimento dos materiais didáticos (produção e reprodução) será de responsabilidade da CONTRATADA. O material deverá conter a descrição dos diversos componentes envolvidos na solução e os manuais de usuários para auxiliá- los na utilização do ambiente e realizar a transferência de tecnologia e passagem de informações técnicas.

4.2.6. Para o PRODERJ o quantitativo de alunos será de no mínimo 08 (oito), para a realização da capacitação, pois além da Gerência de Suporte Técnico que já faz o controle de inventário básico, sem uso de ferramenta específica, outros setores deverão ter acesso à ferramenta, principalmente as gerências de rede, infraestrutura e serviços, banco de dados e de segurança da informação.

4.2.7. As capacitações deverão ser realizadas em dias não intervalados, com exceção dos finais de semana.

4.2.8. A CONTRATADA deverá fornecer certificados de conclusão de capacitação emitidos nos nomes dos colaboradores que o executarem, com no mínimo 75% de presença e participação, cujas cópias deverão ser arquivadas pelo CONTRATANTE para fins de comprovação;

4.2.9. A capacitação deverá ser ministrada, preferencialmente, no decorrer da fase de implementação da solução, a critério do CONTRATANTE e devidamente acordado com a CONTRATADA.

4.2.10. A critério do CONTRATANTE a capacitação poderá ser executada em qualquer fase, desde que esteja na vigência do contrato.

4.2.11. A capacitação deverá ter duração mínima de 16 (dezesseis) horas a serem distribuídas ao longo da semana, ou conforme designado pela CONTRATANTE.

4.2.12. Não será admitida a formação de turmas contendo alunos oriundos de diferentes instituições ou contratos.

4.2.13. Os profissionais responsáveis por ministrar a capacitação deverão conhecer todos os aspectos técnicos e funcionais da solução aqui especificada, com experiência comprovada em capacitações no uso da solução.

4.2.14. A CONTRATADA será responsável pelas despesas relativas à participação de seus instrutores, tais como hospedagem, transporte, diárias, etc.

4.2.15. Se durante o processo de capacitação, a critério da CONTRATANTE, verificar-se o aproveitamento insatisfatório de qualquer dos instrutores, tal fato será comunicado à CONTRATADA que deverá providenciar a substituição do instrutor no prazo máximo de 48 (quarenta e oito) horas após a notificação emitida pelos fiscais do contrato.

4.2.16. As capacitações deverão ser gravadas em vídeoaulas e disponibilizadas ao CONTRATANTE.

4.3. **Requisitos Legais**

4.3.1. **Aplicáveis ao Objeto:**

a) **Adequação à LGPD (Lei Geral de Proteção de Dados – Lei nº 13.709/2018)**

O serviço contratado deve garantir:

- Visibilidade em tempo real de ativos.
- Mapeamento de onde dados pessoais estão armazenados.
- Gestão de patches, segurança e proteção de dados
- Monitoramento de acessos e aplicação de privilégio mínimo.
- Geração de relatórios para auditoria e prestação de contas

b) **Conformidade com a Lei nº 12.965/2014 (Marco Civil da Internet)**

- Garantia da privacidade, integridade e inviolabilidade dos dados de autenticação;
- Registros de acesso devem ser armazenados de forma segura, com proteção contra vazamentos (Art. 13 e 14).

c) **Requisitos de Segurança da Informação (Normas Técnicas e Padrões)**

- ISO/IEC 27001 e 27002 – padrões internacionais para gestão da segurança da informação;
  NIST SP 800-63 – diretrizes de autenticação digital;
- RFCs de autenticação e criptografia, como OAuth 2.0, SAML, OpenID Connect, etc.;
- Autenticação multifator (MFA) ou equivalente em sistemas críticos.
- Decreto nº 48.8891/2024/2024

4.4. **Requisitos de Manutenção**

4.4.1. Não obstante a operacionalização da solução seja exercida pelo CONTRATANTE, todas as rotinas para fins de manutenção com vistas ao pleno e adequado funcionamento da solução ao longo da vigência contratual na garantia de 36 (trinta e seis) meses, serão exercidas pela CONTRATADA, sem ônus para o contratante.

4.4.2. O fornecedor deve disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções.

4.4.3. A CONTRATADA deverá documentar e notificar por escrito as ocorrências sobre eventuais imperfeições, falhas ou irregularidades constatadas na execução dos serviços.

4.4.4. A identificação e a comunicação de defeitos dos produtos deverão ser efetuadas dentro do período de garantia e a totalidade dos defeitos reportados deverá ser corrigida pela CONTRATADA.

4.4.5. A assistência técnica corretiva deverá ser realizada sempre que solicitada pelo CONTRATANTE, por meio da abertura de chamado técnico, para acionamento direto da CONTRATADA, observando-se o tempo de início do atendimento e a severidade da ocorrência para fixação dos níveis de serviço.

4.4.6. A resolução de chamados de suporte técnico que necessitem de intervenção direta no ambiente físico do CONTRATANTE deverá ser precedida de planejamento e somente poderá ser implementada em horário comercial com a devida autorização do CONTRATANTE, desde que precedida pela avaliação dos impactos.

4.4.7. Nos atendimentos aos chamados técnicos abertos, deverá ser disponibilizado suporte técnico personalizado por analista designado como especialista no software, via atendimento (suporte remoto).

4.5. **Requisitos Temporais**

4.5.1. Conforme cronograma previsto no item **"Prazos e condições de entrega dos serviços"** deste documento.

4.6. **Requisitos de Metodologia de Trabalho**

4.6.1. A equipe a ser disponibilizada pelo fornecedor para prestação de todos os serviços deverá seguir as melhores práticas de mercado para cumprimento das atividades objeto da contratação.

4.6.2. As atividades a serem desenvolvidas pela CONTRATADA possuem os seguintes requisitos:

4.6.3. Deverão ser realizadas respeitando o horário de funcionamento de cada local do CONTRATANTE.

4.6.4. Por demanda do CONTRATANTE, poderão sofrer alterações de cronograma dos serviços, desde que não impliquem custos adicionais para a CONTRATADA.

4.6.5. Durante a vigência do contrato, o CONTRATANTE poderá realizar, conforme seu critério, reuniões técnicas e gerenciais com a CONTRATADA, a fim de analisar as entregas das demandas requisitadas pela Administração, definindo as prioridades e estabelecendo um acordo de esforço e prazo para seu atendimento.

4.6.6. São instrumentos formais de comunicação entre o CONTRATANTE e a CONTRATADA:

a) Autorização de Fornecimento;

b) Ordem de Serviço;

c) Plano de Inserção;

d) Termos de Recebimento;

e) Chamado registrado na Central de Atendimento;

f) Ofícios;

g) Relatórios e Atas de Reunião;

h) E-mail; e

i) Demais Termos previstos no instrumento convocatório.

4.6.7. A comunicação entre o CONTRATANTE e a CONTRATADA, para fins de encaminhamento de Autorização de Fornecimento ou Ordem de Serviço, ocorrerá sempre por intermédio do preposto, ou seu substituto, designado pela CONTRATADA.

4.6.8. A comunicação dos usuários com a Central de Atendimento/Suporte da CONTRATADA poderá ser realizada por meio de abertura de chamado via telefone com registro de protocolo ou utilização de sistema informatizado que permita o registro da demanda.

4.7. **Dos Requisitos de Privacidade e Proteção de Dados Pessoais**

4.7.1. **Dados Tratados e de Uso Compartilhado**

4.7.1.1. **Dados Compartilhados**: O tratamento de dados no escopo deste projeto poderá ser utilizado para fins de capacitação, acesso a dados e controle centralizado dos ativos corporativos, com visibilidade em tempo real dos dispositivos, aplicação automatizada de políticas, remoção de softwares não autorizados, redução do risco de perda de dados por meio de criptografia e conformidade regulatória.

4.7.1.2. A execução do projeto segue rigorosamente os princípios da Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018), garantindo que todos os processos envolvendo dados pessoais sejam conduzidos com transparência, segurança e minimização de riscos.

4.7.1.3. O compartilhamento de dados tem como objetivos garantir a segurança cibernética e a proteção dos sistemas contra acessos não autorizados, fraudes e sequestros de sessões, é importante ressaltar que o tratamento dos dados pessoais estará sempre alinhado com a LGPD, garantindo a segurança e a

privacidade das informações dos cidadãos.

4.7.2. **Finalidade do Tratamento e Compartilhamento**

4.7.2.1. Os dados poderão ser utilizados para fins de capacitação, e prevenir e combater ameaças cibernéticas, garantir a integridade dos sistemas e a confidencialidade das informações, e manter a conformidade com as leis de proteção de dados. É importante frisar que o tratamento dos dados pessoais devem estar sempre alinhado com a legislação de proteção de dados, garantindo a privacidade e a segurança das informações dos cidadãos em conformidade com a LGPD.

4.8. **Requisitos de Sustentabilidade Ambiental**

4.8.1. A contratação não trará impactos ambientais significativos, por se tratar de licenças digitais, não se faz necessário declaração de não ofertar produtos com materiais perigosos.

4.8.2. A CONTRATADA deverá priorizar, para a execução dos contratos, a utilização de bens que sejam – no todo ou em partes – compostos por materiais recicláveis, atóxicos e biodegradáveis.

4.8.3. Não se aplicam requisitos sociais e culturais para esta contratação.

4.9. **De Arquitetura Tecnológica**

4.9.1. Considerando que se trata de um serviço SaaS, a arquitetura tecnológica, incluindo hardware e software, será inteiramente gerenciada pela CONTRATADA.

4.9.2. A CONTRATADA será responsável por garantir a interoperabilidade com os ambientes do CONTRATANTE, realizar os interfaceamentos necessários e atender a todas as demais exigências para a perfeita implantação e prestação dos serviços.

4.9.3. Todos os requisitos tecnológicos da solução estão detalhados no ANEXO I - Especificações Técnicas do Objeto.

4.10. **De Projeto e da Implantação**

4.10.1. Será fornecido na modalidade de SaaS (Software as a Service), instalado em data center da CONTRATADA, todos os processos de implementação deverão seguir boas práticas de gestão e segurança da informação, garantindo a correta implantação, configuração e operacionalização da solução contratada. A execução deverá ocorrer preferencialmente por meio de metodologia ágil, assegurando flexibilidade, eficiência e rápida adaptação às necessidades do CONTRATANTE. O processo incluirá a elaboração completa da documentação técnica, garantindo a sustentação e continuidade dos serviços durante e após a vigência do contrato.

4.10.2. Todas as informações, que servem como base para a implantação da solução SaaS e a conformidade com os requisitos contratados, bem como as especificações técnicas e das diretrizes necessárias para a execução do projeto estão descritas no ANEXO I.

4.11. **Das atualizações do sistema**

4.11.1. Sempre que houver o lançamento de nova versão do sistema ou correções de segurança que possam comprometer os serviços prestados, o CONTRATANTE deverá ser notificada com antecedência e a atualização do sistema providenciada pela CONTRATADA, sem custos adicionais ou impactos para o CONTRATANTE. Atualizações que não sejam motivadas por erros ou problemas de segurança só poderão ser realizadas das 23:00 às 06:00 nos dias úteis ou nos fins de semana e feriados.

4.12. **Demais requisitos necessários e suficientes à escolha da solução de gerenciamento unificado de ativos em nuvem**

4.12.1. O serviço deve incluir o fornecimento e instalação de licenças, agentes e quaisquer componentes necessários ao pleno funcionamento da solução, além de prover a interface de gerenciamento centralizado na nuvem, com a devida configuração local quando necessária.

4.12.2. **Exigência de Credenciamento**

4.12.2.1. A qualidade de revenda ou distribuidor autorizado é condição indispensável para a entrega do objeto. Isso se dá porquanto os fabricantes restringem a venda e manutenção de seus produtos apenas aos canais devidamente autorizados.

4.12.2.2. Esta é uma prática extremamente comum no mercado de TI. Através desta exigência, os fabricantes visam assegurar qualidade no serviço de implantação de suas soluções.

4.12.2.3. Diante das considerações expostas, entende-se que é preciso exigir a apresentação de declaração do fabricante da solução informando que a empresa é autorizada a comercializar licenças e prestar serviços de garantia de atualização e funcionamento dos softwares solicitados.

4.12.2.4. Demais requisitos estão detalhados no ANEXO I - Especificações Técnicas do Objeto.

4.12.2.5. A apresentação da Carta de Credenciamento ocorrerá após a homologação e precederá a contratação que estará condicionada à apresentação da carta de credenciamento.

4.12.2.6. Diante das considerações expostas, entende-se que é preciso exigir o credenciamento da empresa junto ao fabricante, contudo, apenas da empresa vencedora do certame, na etapa que visa a assinatura de instrumento contratual, após a homologação, oriundo da ata de registro de preços, neste feito. A não apresentação da carta de credenciamento implicará a desclassificação da empresa vencedora e será chamada a empresa 2ª colocada no certame, e assim sucessivamente, até que a presente exigência seja efetivamente cumprida.

4.13. **De Garantia**

4.13.1. Define-se nesta documentação a garantia, o atendimento necessário para os chamados a complementação de configuração, dúvidas técnicas, operacionais e procedimentais para a solução proposta.

4.13.2. A CONTRATADA deverá realizar toda e qualquer configuração na solução, conforme solicitação da CONTRATANTE, seja on-site ou de forma remota, estando obrigada a esclarecer dúvidas técnicas, operacionais, procedimentais, aos usuários da equipe técnica da CONTRATANTE;

4.13.3. A assistência técnica corretiva será realizada sempre que solicitada pela CONTRATANTE por meio de abertura de chamado técnico, acionando diretamente a CONTRATADA;

4.13.4. A resolução de chamados de Suporte Técnico que necessitem de intervenção direta nos ambientes da CONTRATANTE deverá ser precedida de planejamento e somente poderá ser implementada no ambiente, fora do horário de produção e após avaliação do impacto;

4.13.5. Se houver lançamento de uma nova versão de sistema operacional que faça correções de segurança, a CONTRATADA deve informar à CONTRATANTE e proceder a atualização da solução;

4.13.6. A garantia inclui também a validade técnica, conforme definido na Lei Federal nº 9.609/98, no que concerne a possíveis modificações tecnológicas tais como, mas não exclusivamente:

a) Atualizações de versão e correções de erros;

b) Acesso para downloads de patches, drivers, atualização de software e quaisquer outras atualizações de softwares necessárias, que devem estar disponíveis no website do fabricante da solução, sem custos adicionais ao CONTRATANTE, durante todo o período de garantia;

c) Em caso de o software adquirido/contratado ser descontinuado durante o período de vigência contratual, a empresa CONTRATADA deverá fornecer a nova versão do produto equivalente, na mesma quantidade estabelecida em contrato, de modo a garantir a continuidade da solução;

d) Vulnerabilidades (SQL Injection, etc);

e) Sistemas operacionais, servidores de aplicações, etc., sendo tratadas como manutenções eventuais as modificações tecnológicas (por força da Lei 9.609/98); e

f) Disponibilizar as revisões dos manuais técnicos e/ou documentação dos softwares licenciados.

4.13.7. A garantia deverá:

a) Permitir a abertura, acompanhamento e validação de chamados através de e-mail e/ou website (portal do cidadão) e/ou telefone (0800) no regime 24x7x365, com atendimento em português;

b) Possuir canal com os fabricantes envolvidos na solução dos incidentes, bem como ser responsável pela abertura e acompanhamento dos chamados junto aos mesmos;

c) Possuir os processos de gerenciamento de incidentes, requisição, eventos, problemas, mudanças, incidentes críticos e atendimento aos usuários;

d) Suporte técnico de 2º nível quanto a dúvidas de customização e configuração do equipamento e console de gerenciamento.

4.13.8. Na abertura de chamados técnicos serão fornecidas informações pela CONTRATANTE, como:

a) Anormalidade observada;

b) Nome do responsável pela solicitação do chamado técnico;

c) Sistema/versão/módulo/item;

d) Natureza do problema;

e) Descrição da natureza enfrentada.

4.13.9. O atendimento técnico deverá atender os seguintes requisitos técnicos:

a) As solicitações de atendimento de suporte, só poderão ser realizadas pelos contatos cadastrados, em qualquer horário por e-mail e telefone;

b) O atendimento remoto de Suporte e Monitoramento pelos canais: telefônico ou web ou e-mail, funcionará em regime 24 horas por dia, 7 dias por semana para incidentes e solicitações elegíveis de se resolver remotamente;

c) O atendimento presencial de Suporte de incidentes e solicitações elegíveis de se resolver presencialmente funcionará, preferencialmente, no horário comercial das 9:00h às 18:00h. Exceto quando o suporte for emergencial. Nestes casos, o atendimento deverá ser fora do horário comercial em regime 24x7.

4.13.10. A CONTRATADA, após a realização do suporte, deverá apresentar os Relatórios contendo:

a) Identificação do chamado;

b) Data e hora do início e término do atendimento com a solução do chamado técnico;

c) Identificação do defeito;

d) Técnico responsável pela solução do defeito, as providências adotadas, origem do problema e outras informações pertinentes;

e) Atualizações de software/versões realizadas;

f) Acionamentos feitos à equipe da CONTRATADA;

g) Relatórios Extraordinários.

4.13.11. A manutenção corretiva ocorrerá de falha de funcionalidades ou de recursos do sistema, de qualquer natureza, detectada pelo usuário, ou seja, em desacordo com as funcionalidades definidas nas telas, nas regras de negócio, nos relatórios, interfaces com outros sistemas, dentre outras. Tais falhas devem ser classificadas, pelo usuário, observando a GRAVIDADE e a URGÊNCIA e conforme essa definição será feito a priorização, conforme acordo de nível de serviço deste documento.

4.13.12. A CONTRATANTE poderá solicitar, sem qualquer ônus adicional, a substituição ou correção da solução de software, quando se verificarem vícios, defeitos ou incorreções.

4.13.13. Os profissionais deverão fornecer suporte técnico e operacional necessários ao bom funcionamento do sistema, envolvendo os seguintes serviços:

a) Dirimir dúvidas e resolver problemas relativos às características técnicas, funcionamento lógico e físico do sistema.

b) Fazer avaliação e emitir parecer técnico em situações anormais de funcionamento do sistema.

c) Prestar assessoria para adequação do sistema à legislação vigente.

d) Simulações deverão ser efetuadas em paralelo, isto é, mantendo íntegros os dados do cadastro do sistema. A CONTRATADA deverá prover ambiente com cópia integral da base de dados para testes, simulações e homologações para áreas da Contratante, sempre que necessário.

e) Acionar equipe necessária para solução de questões em que os servidores indicados pela Contratante não tenham condições de atender no que diz respeito à operação e configurações do sistema.

4.13.14. A garantia se configura em aspecto agregado à solução, cujo lapso temporal não se confunde com o lapso de vigência do contrato.

4.13.15. A garantia deverá ser de 36 (trinta e seis) meses, a contar da emissão do termo de recebimento definitivo, ou do prazo estabelecido pelo fabricante, caso este seja maior.

4.13.16. Alterações na legislação vigente que impliquem manutenções no sistema para sua adaptação ou adequação, desde que não alterem estrutura básica dos sistemas, estão incluídas nessa garantia e devem ser executadas, testadas e homologadas em tempo para assegurar que a CONTRATANTE não perca nenhum prazo legal.

4.14. **De Experiência e Formação da Equipe que Executará os Serviços Relacionados à Solução de TIC**

4.14.1. Não se Aplica

4.15. **Requisitos Materiais e Humanos**

4.15.1. Em observação ao entendimento do Enunciado nº 14, item 5 da Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ, saliente-se que o objeto da presente contratação não prevê o uso de mão de obra residente nas dependências dos órgãos e entidades CONTRATANTES.

4.15.2. Não será necessária a utilização de mão de obra especializada, tendo em vista que os recursos humanos necessários à instalação e configuração da solução, bem como responsáveis pelas manutenções preventivas e corretivas, já fazem parte do escopo do objeto e não será contratado como item específico.

4.16. **Necessidades de Adequações no Ambiente**

Trata-se de uma solução a ser instalada na infraestrutura da CONTRATADA, portanto não há necessidade de adequações no ambiente do CONTRATANTE.

4.16.1. Por se tratar de um modelo baseado em nuvem, que dispensa a instalação local de softwares, o SaaS contribui para a redução da complexidade técnica e do uso de recursos físicos no ambiente da CONTRATANTE.

4.16.2. É importante ressaltar que esse tipo de contratação, além de aliviar o ambiente da CONTRATANTE, oferece uma forma mais flexível, acessível e eficiente de utilizar software. Ao eliminar a necessidade de instalar e manter software localmente, o SaaS permite que a CONTRATANTE se concentre em seu negócio.

4.16.3. Demais especificações no anexo Técnico, conforme especificado no ANEXO I.

4.17. **Reunião de kick-off**

4.17.1. Será realizada reunião de kick-off, conforme especificado no ANEXO I.

5. **LEVANTAMENTO DE MERCADO**

5.1. A análise comparativa de soluções, consideradas as disposições do art. 7º e art. 9º, ambos do Decreto Estadual nº 48.816/2023, bem como as orientações da Nota Técnica TCE-RJ nº 06/2023, visa elencar as alternativas de atendimento à demanda, considerando, além do aspecto econômico, os aspectos qualitativos em termos de benefícios para o alcance dos objetivos da contratação.

5.2. Para fins de atendimento da presente demanda, foi realizado uma pesquisa em que foram encontradas potenciais soluções para atendimento da demanda demonstrada abaixo:

5.3. Nesta seção, pretende-se apresentar os aspectos relacionados ao mercado fornecedor, apontando suas principais características e especificidades relacionadas às compras de governo nesse segmento.

5.4. A equipe de planejamento seguiu uma ordem lógica, que permitiu registrar todo o esforço empreendido até a escolha da solução que atende a demanda de forma mais eficiente.

5.5. Em primeiro lugar, a equipe de planejamento buscou entender o objeto junto ao segmento de mercado. Posteriormente, buscou avaliar as alternativas que se encontram disponíveis e, por fim, buscou avaliar qual o melhor modelo de fornecimento do objeto. A partir desses insumos, a equipe analisou todos os prós e contras dos insumos provenientes das análises acima e cotejou com a demanda identificada pela Área Requisitante, o que permitiu concluir pelo cenário que atende às necessidades de forma mais eficiente.

5.6. O segmento de soluções de gerenciamento de ativos em nuvem compreende um tipo de objeto de extrema relevância para proteção do ambiente tecnológico. Esse segmento de mercado é amplo, existindo ferramentas de diversos fabricantes com funcionalidades e modelos distintos, os quais passaremos a analisar no tópico a seguir.

5.7. As alternativas consideradas foram:

- **Desenvolvimento interno:** considerado inviável por falta de equipe técnica especializada e tempo de entrega incompatível.
- **Soluções isoladas (softwares livres):** considerado inviável por custos de integração, baixa eficiência e complexidade operacional.
- **Soluções unificadas prontas:** recomendáveis por agregarem valor integrado e escalabilidade comprovada no setor público.

5.7.1. Dentre as soluções unificadas, passaremos a analisar as mais relevantes nos tópicos a seguir:

5.7.2. **Solução 1**

5.7.2.1. Esta solução oferece uma abordagem abrangente para a gestão de endpoints, consolidando diversas funcionalidades essenciais em uma única plataforma. Com cobertura completa, abrange inventário de ativos, conformidade e políticas, resposta a incidentes e gestão da experiência digital, proporcionando visibilidade e controle total sobre os dispositivos da organização

5.7.2.2. Sua **plataforma unificada** integra ferramentas de EDR (Endpoint Detection and Response), IR (Incident Response), gerenciamento de patches e inventário de ativos, eliminando a necessidade de múltiplas soluções isoladas e melhorando a eficiência operacional e a segurança.

5.7.2.3. O fabricante desta solução é Tanium.

5.7.3. **Solução 2**

5.7.3.1. É uma solução corporativa de gestão e inventário automatizado de ativos, sua arquitetura em nuvem permite escalabilidade, atualizações automáticas e alta disponibilidade, com cobertura para ambientes híbridos. A solução é comercializada por meio de licenciamento corporativo, com módulos que podem ser contratados conforme as necessidades da organização.

5.7.3.2. A implementação da solução é realizada por parceiros especializados com a possibilidade de incluir serviços profissionais e treinamentos técnicos.

5.7.3.3. O fabricante desta solução é Qualys.

5.7.4. **Solução 3**

5.7.4.1. É uma solução robusta de gestão de endpoints que abrange funcionalidades como inventário de ativos, aplicação de patches, conformidade com padrões de segurança (como STIG e CIS) e distribuição de software. Voltada para ambientes corporativos, a solução é oferecida com licenciamento enterprise e pode incluir serviços profissionais especializados.

5.7.4.2. A implantação desta solução é realizada por integradores, com garantia técnica contratado e oferta de treinamento técnico para garantir o uso eficiente da plataforma.

5.7.4.3. O fabricante desta solução é BigFix (HCL).

5.7.5 **Solução 4**

5.7.5.1 É uma plataforma de gestão unificada que oferece recursos integrados para gerenciamento de patches, ativos de TI, configurações e administração de endpoints.

5.7.5.2 A solução é implantada por meio de integradores especializados, com disponibilização de treinamento técnico e suporte baseado em acordos de nível de serviço (SLA) contratados, garantindo eficiência e conformidade na gestão de ambientes de TI.

5.7.5.3 O fabricante desta plataforma é Ivanti.

5.8. **Análise Comparativa (Benchmarking)**

1 - Solução 1

- A solução oferece uma abordagem abrangente para a gestão de endpoints, consolidando diversas funcionalidades essenciais em uma única plataforma. Com cobertura completa, a Tanium XEM abrange inventário de ativos, conformidade e políticas, resposta a incidentes e gestão da experiência digital, proporcionando visibilidade e controle total sobre os dispositivos da organização.

Vantagens:

- **Plataforma unificada:** Integra em um só console gestão de endpoints, segurança, visibilidade em tempo real e automação de remediação.
- **Resposta a incidentes em tempo real:** Excelente capacidade de detecção e resposta rápida a ameaças, com visibilidade completa de endpoints.
- **Conformidade e auditoria:** Forte aderência a padrões regulatórios (CIS, NIST), com geração automatizada de relatórios.
- **Experiência digital:** Monitoramento e análise de performance do endpoint com foco na experiência do usuário final.
- **Escalabilidade:** Robusta o suficiente para ambientes complexos e de larga escala, como órgãos públicos.

Desvantagens:

- **Alto custo** de licenciamento inicial e manutenção.
- **Complexidade operacional e**xige equipe com treinamento intensivo.
- **Implantação** via integradores especializados.

2 - Solução 2

- Uma solução corporativa de gestão e inventário automatizado de ativos, sua arquitetura em nuvem permite escalabilidade, atualizações automáticas e alta disponibilidade, com cobertura para ambientes híbridos. A solução é comercializada por meio de licenciamento corporativo, com módulos que podem ser contratados conforme as necessidades da organização.

Vantagens:

- **Plataforma unificada:** Permite descobrir e inventariar automaticamente ativos locais, em nuvem, endpoints e containers com uma visão única e centralizada.
- **Priorização de ameaças:** Prioriza vulnerabilidades realmente relevantes através de um mecanismo de gerenciamento que cruza dados de exploração ativa, criticidade do ativo e inteligência de ameaças.
- **Cobertura híbrida e multicloud nativa:** Suporte a redes locais e ambientes cloud como AWS, Azure, GCP.
- **Normas de conformidade:** Facilita o atendimento a regulamentos e frameworks de segurança, como CIS Benchmarks, NIST, PCI-DSS, ISO 27001 e LGPD

Desvantagens

- **Cobertura limitada de dispositivos offline ou isolados:** Depende de conectividade para execução de varreduras e coleta contínua que pode dificultar a cobertura de ativos em redes segregadas ou desconectadas.
- **Sem foco em DEX:** Não possui recursos nativos voltados à experiência do usuário final, como monitoramento de desempenho de aplicativos ou análise de uso.
- **Customizações complexas:** Fluxos personalizados como ações de resposta ou relatórios detalhados podem depender de conhecimento avançado de scripts e APIs, exigindo maior domínio técnico ou apoio do suporte especializado.

3 - Solução 3

- Uma solução robusta de gestão de endpoints, projetada para atender às exigências de ambientes corporativos complexos. A plataforma oferece funcionalidades completas, incluindo inventário detalhado de ativos, aplicação de patches, verificação de conformidade com padrões como STIG e CIS, além da distribuição automatizada de software. Essa abordagem integrada garante maior segurança, visibilidade e controle sobre os dispositivos da organização.

Vantagens:

- **Gestão robusta de endpoints:** Inventário, patch management, compliance (STIG, CIS), e distribuição de software.
- **Automação de segurança:** Correção automática de falhas e não conformidades.
- **Visibilidade unificada:** Permite rastrear e auditar todos os ativos, com foco em conformidade.
- **Escalabilidade comprovada:** Usado amplamente em governos e grandes corporações.

Desvantagens

- **Cobertura limitada de GRC:** Não possui módulos nativos de gestão de risco, governança ou políticas.
- **DEX não priorizada:** Menor foco em experiência digital do usuário final.
- **Interface técnica:** Exige expertise técnica para gestão e operação contínua.

4 - Solução 4

- Uma plataforma de gestão unificada que oferece recursos integrados para gerenciamento de patches, ativos de TI, configurações e administração de endpoints.

Vantagens:

- **Plataforma unificada:** Combina ITSM, gestão de ativos, endpoint management e automação.
- **Componentes de GRC e compliance:** Suporte a políticas, auditorias e conformidade.
- **Foco em DEX:** Recursos de monitoramento da experiência digital do usuário.
- **Automação e integração:** Possui bom nível de orquestração entre áreas de TI e segurança.

Desvantagens

- **Menor profundidade em segurança:** Não é tão forte quanto Tanium ou BigFix na parte de segurança e remediação em tempo real.
- **Componentes GRC são básicos:** Pode ser necessário complementar com plataformas como OneTrust para uma visão completa.
- **Complexidade na customização:** Algumas organizações relatam desafios na configuração inicial em ambientes muito específicos.

5.9. **Avaliação de Mercado**

5.9.1. As soluções de mercado possuem processos sólidos, testados e estabilizados permitindo ganhos de qualidade e produtividade.

5.9.2. Nesse sentido, vislumbramos que as soluções dos fabricantes abaixo relacionados atendem à especificação técnica requerida nessa contratação:

- Solução 1 - Tanium: The Platform for Autonomous Endpoint Management
- Solução 2 - Streamline Risk Management Across Your Enterprise | Qualys
- Solução 3 - Unified Endpoint Management with HCL BigFix | UEM Solutions
- Solução 4 - Ivanti - Everywhere Work. Elevated.

6. ANÁLISE DE PROJETOS SIMILARES

6.1. Foram analisadas contratações similares formalizadas por outros órgãos e entidades, por meio de consultas ao sistema Painel de Preços do Portal de Compras do Governo Federal, com objetivo de identificar a existência de novas metodologias, tecnologias ou inovações que melhor atendessem às necessidades da Administração, e as que foram identificadas foram incorporadas na contratação em análise.

6.2. Na contratação em análise não foram identificadas situações específicas ou casos de complexidade técnica do objeto, que pudessem acarretar a realização consulta pública para coleta de contribuições a fim de definir a solução mais adequada visando preservar a relação custo-benefício, em face dos serviços serem considerados comuns.

6.3. **Análise de Projetos Similares da Solução de Gerenciamento de Ativos**

OBJETO: Solução de Gerenciamento Unificado de Ativos	
ÓRGÃOS E ENTIDADES	**OBJETO**
TRE/SP (110990008)	Contratação de empresa especializada em prestação de serviços da Solução de Gerenciamento de ativos e patches, em nuvem (Cloud Computing), por 24 (vinte e quatro) meses, incluindo a prestação de serviços suporte técnico, implementação e configuração da solução e treinamento. (Grupo 2 e 4 do pregão)
PCDF (110990102)	Contratação de empresa especializada para fornecimento e instalação de solução de gestão e remediação de vulnerabilidades em ativos de tecnologia da informação e aplicações web, incluindo funções de gestão de configurações e certificados digitais, suporte

	24x7 e garantia (manutenção e suporte técnico), por 24 meses

CONTRATAÇÕES SIMILARES	PREGÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL	Atualização pelo ICTI * (7,26% - jan/25	ESTIMATIVA DE CONTRATAÇÃO VALOR MÉDIO TOTAL
TRE/SP (110990008)	ARP Nº 78/2022	2.000	R$ 360 24 meses R$ 540,00 36 meses	R$ 1.080.000,00	R$ 1.158.408,00	**R$ 1.527.000,25**
PCDF (110990102)	Pregão Eletrônico Nº 90.008/2025	2.000	R$ 524,07 24 meses R$ 786,10 36 meses	R$ 1.572.200,00+ R$ 215,595,00 (24 meses) R$ 323.392,50 (36 meses) (suporte técnico) = R$ 1.895.592,50	-	

*Índice de custo da tecnologia da informação (ICTI) - IPEA (Índice e série histórica disponível neste link) **foi aplicado o índice nos pregões com mais de 01 (um) ano.**

6.4. **Análise de Projetos Similares da: Serviço de Instalação para Solução de Gerenciamento Unificado de Ativos**

OBJETO: Serviço de Instalação para Solução de Gerenciamento de Ativos	
ÓRGÃOS E ENTIDADES	**OBJETO**
TRE/SP (110990008)	Serviço de implantação e configuração na infraestrutura do Tribunal
PCDF (110990102)	Serviços de Instalação, Transição e Configuração / Parametrização de Software

CONTRATAÇÕES SIMILARES	PREGÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL	Atualização pelo ICTI * (7,26% - jan/25	ESTIMATIVA DE CONTRATAÇÃO VALOR MÉDIO TOTAL
TRE/SP (110990008)	ARP Nº 78/2022	1	R$ 14.790,22	R$ 14.790,22	R$ 15.863,99	**R$ 22.931,99**
PCDF (110990102)	Pregão Eletrônico Nº 90.008/2025	1	R$ 30.000,00	R$ 30.000,00	-	

*Índice de custo da tecnologia da informação (ICTI) - IPEA (Índice e série histórica disponível neste link) **foi aplicado o índice nos pregões com mais de 01 (um) ano.**

6.5. **Análise de Projetos Similares da: Treinamento para Solução de Gerenciamento Unificado de Ativos**

OBJETO: Treinamento para Solução de Gerenciamento Unificado de Ativos	
ÓRGÃOS E ENTIDADES	**OBJETO**
TRE/SP (110990008)	Serviço de repasse de conhecimento com mínimo de 20 horas
PCDF (110990102)	Treinamento - Instalação / Utilização Equipamento

CONTRATAÇÕES SIMILARES	PREGÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL	Atualização pelo ICTI * (7,26% - jan/25	ESTIMATIVA DE CONTRATAÇÃO VALOR MÉDIO TOTAL
TRE/SP (110990008)	ARP Nº 78/2022	8	R$ 1.155,93	R$ 9.247,44	R$ 9.918,80	**R$ 41.236,44**
PCDF (110990102)	Pregão Eletrônico Nº 90.008/2025	8	R$ 9.069,26	R$ 72.554,08	-	

6.6. **Custo Total de propriedade**

Valor médio das contratações similares para Solução de Gerenciamento Unificado de Ativos: **R$1.527.000,25**
+
Serviço de Instalação da Solução: **R$ R$ 22.931,99**
+
Treinamento para Solução de Gerenciamento Unificado de Ativos: **R$ 41.236,44**
=
Valor total médio das contratações similares: **R$ 1.591.168,68**

6.7. **Análise Comparativa de Propriedade**

6.7.1. A seguir apresentaremos um quadro comparativo entre as possíveis soluções apresentadas:

Requisitos	**Cenários - Análise de Viabilidade das Soluções**			
	Solução 1	**Solução 2**	**Solução 3**	**Solução 4**
Abrangência Funcional	Muito alta – Gestão, segurança, DEX, remediação	Foco em gestão de vulnerabilidades e ameaças	Forte em gestão técnica e compliance	Abrangente – ITSM, DEX, GRC leve
Capacidade GRC (Governança, Risco e Conformidade)	Compliance técnico forte, GRC via integração	Básica – apenas suporte a processos	Limitada a compliance técnico	Moderada – GRC funcional
Resposta a Incidentes	Reação em tempo real e remediação imediata	Boa – apoio à resposta a incidentes	Técnica – sem camada de atendimento	Boa – com automação de processos de resposta
Experiência Digital (DEX)	Avançada – monitoramento contínuo do usuário	Fraca — não contempla monitoramento, análise e otimização da experiência digital dos usuários	Sem foco específico	Inclusa – com foco em experiência do usuário
Gestão de Endpoints (TI Operacional)	Completa e em tempo real	Básica — atende bem ao inventário, conformidade e aplicação de patches	Completa – forte em patch/configuração	Completa – gestão unificada
Escalabilidade	Alta – Arquitetura distribuída peer-to-peer	Alta — escalável para ambientes de grande porte	Alta – usado em grandes governos	Alta – depende de configuração
Integração com outras plataformas	Flexível – APIs abertas, SIEM, GRC, ITSM	Ampla – APIs RESTful, SIEMs, ITSMs, plataformas cloud e ferramentas de automação	Integrações técnicas via agente	Ampla – com ServiceNow, Microsoft, etc.
Facilidade de Implantação	Requer capacitação técnica e projeto bem definido	Requer capacitação técnica, apoio externo e planejamento mais profundo em ambientes complexos	Implantação técnica	Suporte via parceiros locais
Custo estimado (licença e operação)	Elevado – solução premium	Alta — custo de licenciamento e operações significativas	Médio a alto	Médio, com bom custo-benefício
Aderência ao Setor Público	Alta	Usado mais em help desks corporativos	Alta	Alta
Resultado da Análise	**Altamente viável**	**Altamente viável**	**Viável com ressalvas**	**Viável com ressalvas**

7. **MÉTRICA PARA MENSURAÇÃO DOS SERVIÇOS**

7.1. Por se tratar de uma solução disponibilizada na modalidade SaaS (Software as a Service), cuja contratação ocorre por meio de subscrição de licenças de uso, não se aplica a utilização de métricas tradicionais de mensuração de serviços, como volume de dados processados, quantidade de acessos ou tempo de utilização.

7.2. A mensuração será realizada com base na disponibilização e no pleno funcionamento da solução contratada, abrangendo todas as funcionalidades previstas no escopo, sem limitação de volume de dados, acessos ou transações, durante a vigência da contratação. O Serviço será considerado adequado quando a solução estiver disponível, operante e entregando os resultados esperados no que se refere ao inventário e gerenciamento de ativos, conforme especificações técnicas estabelecidas neste documento.

8. JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO

8.1. Levando em conta os aspectos de eficiência e padronização, bem como práticas de mercado, não resta dúvida que a melhor opção para resolver o problema de negócio enfrentado pela Administração Pública e demonstrado nesse Estudo Técnico, é a contratação de licenciamento/subscrição de uma solução unificada em nuvem com garantia de 36 (trinta e seis) meses.

8.2. O segmento de soluções de gerenciamento de ativos em nuvem compreende um tipo de objeto de extrema relevância para proteção do ambiente tecnológico. Sendo imprescindível que os dados tratados em ambiente de nuvem sejam armazenados em data centers localizados em território brasileiro, admitindo-se o tratamento de dados em data centers fora do território brasileiro somente nos casos em que haja cópia de segurança atualizada armazenada em data centers localizados em território brasileiro.

8.3. Dentre as alternativas de mercado analisadas, as soluções unificadas prontas demonstraram ser altamente viáveis e recomendáveis visto o valor integrado e escalabilidade comprovada no setor público.

9. ESTIMATIVA DAS QUANTIDADES

9.1. A definição precisa do quantitativo necessário para a contratação está intrinsecamente ligada aos resultados e conclusões do Estudo Técnico Preliminar (ETP). A elaboração do ETP é essencial para determinar as especificações técnicas, a viabilidade e a melhor solução para atender à demanda, o que, por sua vez, impactará diretamente na quantidade de bens ou serviços a serem contratados. Portanto, a definição do quantitativo será realizada após a conclusão da **Intenção de Registro de Preço (IRP)**, garantindo a precisão e a adequação da contratação às necessidades da administração pública.

ITEM	ID SIGA	ID PCA	ESPECIFICAÇÃO DO OBJETO	MÉTRICA	FORMA DE FORNECIMENTO	QUANTIDADE ESTIMADA
1	195070	24635	Subscrição de licenças de gerenciamento unificado de ativos baseada em nuvem, com garantia de 36 meses, incluindo o serviço de instalação da solução e o treinamento especializado	Unidade	Subscrição licença por 36 meses	2000

9.2. **Item 1**

9.3. **Subscrição de licenças de Gerenciamento Unificado de Ativos.**

9.3.1. A subscrição de licenças de gerenciamento unificado de ativos consiste em uma solução baseada em nuvem que permite o controle centralizado sobre os ativos corporativos e a visibilidade em tempo real, aprimorando os processos de auditoria e investigação, aplicação automatizada de políticas, remoção de softwares não autorizados e desativação de serviços em desuso, promovendo maior eficiência operacional e aderência aos padrões estabelecidos. Também busca mitigar a disseminação de códigos maliciosos com a aplicação contínua de patches de segurança e o gerenciamento preciso do inventário de software e hardware. Por estar hospedada na nuvem, a solução oferece alta escalabilidade, rápida implementação e dispensa a necessidade de infraestrutura local, tornando a proteção contra fraudes mais ágil, eficiente e acessível

9.3.2. Cada subscrição corresponde a um dispositivo físico ou virtual (desktop, laptop, servidor, container, hypervisor etc.) onde a solução seja instalada ou capaz de processar dados. No caso de sistema virtualizado, admite-se que o hypervisor conte como uma instância adicional além das máquinas virtuais gerenciadas. A demanda do PRODERJ foi estimada em 2000 subscrições, tomando como base no número total de ativos passíveis de serem inventariados em utilização pelo PRODERJ.

9.4. **Serviço de Instalação da Solução de Gerenciamento Unificado de Ativos em nuvem**

9.5. O prazo para a instalação da instância dedicada à CONTRATANTE é de 30 dias corridos, após Ordem de Serviço. Deve ser entregue ambiente SaaS totalmente funcional e com fornecimento das credenciais de acesso dentro do prazo especificado.

9.6. **Treinamento para Solução de Gerenciamento Unificado de Ativos em nuvem**

9.6.1. Se faz necessário para capacitar a equipe interna da CONTRATANTE para operar a ferramenta.

9.6.2. O quantitativo de alunos que realizarão a capacitação estão justificados com base no item 4.2.6.

9.6.3. Todos os Requisitos e Especificações Técnicas da Solução estão descritos no Anexo I.

10. ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO

10.1. Projetos similares realizados por outros órgãos da Administração Pública, foi realizada a pesquisa no catálogo de soluções de TIC da secretaria de governo digital da secretaria especial de desburocratização gestão e governo digital do ME e não encontramos contratações similares no referido Catálogo de Soluções de TIC.

10.2. O valor estimado para esta contratação é de **R$ 1.591.168,68** (um milhão, quinhentos e noventa e um mil cento e sessenta e oito reais e sessenta e oito centavos) baseado na tabela do item "**Análise da Comparativa do Custo Total de Propriedade"**, conforme descrito abaixo:

10.3.

10.4.

ITEM	ESPECIFICAÇÃO DO OBJETO	QTD	VALOR MÉDIO UNITÁRIO	VALOR MÉDIO GLOBAL
1	Subscrição de licenças de gerenciamento unificado de ativos baseada em nuvem, com garantia de 36 meses, incluindo o serviço de instalação da solução e o treinamento especializado	2000	**R$ 795,58**	**R$ 1.591.168,68**

OBS: Para se chegar no valor unitário foi realizado a divisão do valor de R$ 1.591.168,68 pela quantidade de 2.000 para encontrar o valor médio unitário da solução contemplando a subscrição de licenças, o serviço de instalação da solução e o treinamento especializado.

11. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

11.1. Trata-se de Contratação de empresa especializada fornecimento de Subscrição de licenças de gerenciamento unificado de ativos baseada em nuvem, com garantia de 36 meses, o serviço de instalação da solução e o treinamento especializado, conforme condições definidas no ANEXO I, deste documento.

11.2. O ciclo de vida das soluções tratadas neste documento contempla as seguintes fases: Contratação, Integração Técnica, Configuração de Regras e Lógica de Negócio, Garantia Técnica e Atualizações, Treinamento, Avaliação e Otimização e Renovação ou Encerramento.

11.3. Esse ciclo pode se repetir de forma contínua, especialmente nas fases de garantia e otimização, que são recorrentes durante todo o período de subscrição.

12. NATUREZA DO OBJETO DA CONTRATAÇÃO

12.1. Trata-se do objeto de serviço de ***natureza comum***, uma vez que os seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

12.2. A prestação de serviços será de ***natureza continuada***, pois visa atender à necessidade pública de forma permanente e contínua, por mais de um exercício financeiro, assegurando a integridade do patrimônio público e o funcionamento das atividades do órgão ou entidade, de modo que sua interrupção possa comprometer a prestação de um serviço público ou o cumprimento da missão institucional.

13. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

13.1. A Subscrição de licenças de gerenciamento unificado de ativos baseada em nuvem, com garantia de 36 meses, o serviço de instalação da solução e o treinamento especializado para sua utilização compõem um conjunto único e indivisível, intrinsecamente ligado e essencial para assegurar a integridade, confiabilidade e continuidade das operações da organização. O fracionamento desses elementos em itens distintos comprometeria a eficácia global da solução, dificultaria a integração entre software, serviços e capacitação, além de introduzir riscos inaceitáveis de descontinuidade e ineficiências operacionais. Dessa forma, justifica-se a contratação de forma aglutinada em item único, garantindo-se a plena efetividade da solução a ser implantada.

13.2. A análise das especificações técnicas e nuances de comercialização no mercado evidenciam que a solução em pauta é composta por componentes indivisíveis que não podem ser adquiridos separadamente, sem comprometer a funcionalidade da solução. Assim, torna-se inviável a contratação de diversos fornecedores sem prejuízo técnico.

13.3. Trata-se de uma solução integrada, cujos componentes (infraestrutura, plataforma e suporte) são interdependentes e prestados de forma contínua por um único fornecedor, conforme as condições técnicas e comerciais previamente estabelecidas no instrumento de registro de preços.

13.4. O parcelamento, neste caso, comprometeria a eficiência da contratação, gerando riscos à interoperabilidade, ao suporte técnico unificado e à gestão contratual. Assim, a contratação do objeto de forma única se mostra mais vantajosa e tecnicamente adequada, em conformidade com os princípios da economicidade, eficiência e padronização.

13.5. Importa destacar que, conforme prevê o art. 40, §2° da Lei n° 14.133/2021, o parcelamento deve ser considerado técnica e economicamente viável, mas o §3° excepciona essa regra quando houver risco de comprometimento da eficiência técnica, perda de economia de escala ou ameaça à integridade do objeto:

> *"§ 2º Na aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:*
>
> *I - a viabilidade da divisão do objeto em lotes;*
> *II - o aproveitamento das peculiaridades do mercado local, com vistas à economicidade, sempre que possível, desde que atendidos os parâmetros de qualidade; e*
> *III - o dever de buscar a ampliação da competição e de evitar a concentração de mercado.*
>
> *§ 3º O parcelamento não será adotado quando:*
>
> *I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;*
> *II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;*
> *III - o processo de padronização ou de escolha de marca levar a fornecedor exclusivo."*

13.6. O modelo de contratação em item único se justifica por razões técnicas amplamente reconhecidas no setor de TIC. Tais motivos incluem:

- a interdependência funcional entre os módulos a serem contratados, que compartilham recursos de configuração, autenticação, repositórios de dados e integração com o ambiente já existente;
- a necessidade de um ambiente técnico homogêneo, no qual a instalação e parametrização sejam realizadas com pleno domínio da infraestrutura atual e dos padrões técnicos da organização, o que exige visão global da arquitetura da solução;
- a conveniência e segurança na manutenção da responsabilidade técnica e única indivisível pela entrega, configuração, suporte e evolução da solução, evitando sobreposição de obrigações ou lacunas de atendimento em caso de falhas técnicas;
- a natureza dos treinamentos previstos, que são acoplados à configuração técnica específica da solução instalada, de modo que capacitações realizadas por empresa distinta da instaladora comprometem o aproveitamento pedagógico e a aplicabilidade prática;
- a necessidade de gestão centralizada e segura de credenciais, acessos e integrações, em conformidade com os padrões de segurança das informações adotadas, o que seria inviabilizado pela fragmentação da execução entre fornecedores distintos;
- e ainda, a exigência de padrões de suporte e atualização unificados, que garantam a compatibilidade entre os módulos em ciclos de manutenção preventiva e corretiva, o que somente é possível por meio da gestão técnica centralizada.

13.7. O Tribunal de Contas da União, especialmente por meio da Súmula n° 247/TCU, reforça esse entendimento:

> *"É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala (...)".*

13.8. Nesse caso, haverá evidente prejuízo técnico na fragmentação da contratação, considerando que os módulos e serviços são inseparáveis do ponto de vista funcional e a execução isolada por empresas diferentes comprometeria a compatibilidade entre os componentes, a integridade da solução, a efetividade dos treinamentos e a uniformidade do suporte técnico.

13.9. Nesse contexto, a dinâmica contratual requer um cenário de interdependência e interoperabilidade.

13.10. Uma possível apuração de falhas na prestação dos serviços num sistema que requer a dinâmica da interdependência e interoperabilidade seria complexa e impactaria a continuidade da sua execução, caso a adjudicação ocorresse por itens. A apuração de responsabilidade em eventual inexecução contratual demandaria tempo e comprometeria a entrega do objeto, caso nenhum dos contratados assumisse a responsabilidade e se comprometesse com a resolução. Nessa linha, o risco de paralisação do serviço se eleva sobremaneira, o que pode ser eliminado com adjudicação na forma global.

13.11. Portanto, a contratação em item único é tecnicamente necessária e juridicamente admissível, não configurando aglutinação indevida, tampouco restrição à competitividade, pois há no mercado empresas plenamente aptas a fornecer a totalidade do objeto, desde que devidamente homologadas e autorizadas pelo fabricante da solução.

14. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

14.1. A presente demanda visa a contratação de empresas para prestação de serviços de licenciamento Subscrição de licenças de gerenciamento unificado de ativos baseada em nuvem, com garantia de 36 meses, o serviço de instalação da solução e o treinamento especializado, com o objetivo de auxiliar o PRODERJ e demais órgãos da Administração Pública a proteção dos ativos de TIC contra diferentes tipos de intercorrências que possam comprometer seu funcionamento e disponibilidade, bem como obter os seguintes benefícios:

- **Estabelecer controle centralizado sobre os ativos corporativos, permitindo visibilidade em tempo real dos dispositivos conectados à rede e seus respectivos estados de conformidade**
- **Aprimorar a configuração e o gerenciamento dos dispositivos por meio da aplicação automatizada de políticas, remoção de softwares não autorizados e desativação de serviços em desuso, visando maior eficiência operacional e conformidade com os padrões estabelecidos.**
- **Mitigar a disseminação códigos maliciosos, aplicando correções de segurança (patches) de forma contínua e gerenciando o inventário de software e hardware com precisão.**
- **Auxiliar na conformidade com normativas e boas práticas de segurança da informação, como as diretrizes do Programa de Privacidade e Segurança da Informação (PPSI), garantindo a rastreabilidade das ações executadas nos endpoints.**
- **Aumentar a eficiência operacional da área de TI, através da automação de tarefas de configuração, inventário, atualizações e resposta a incidentes.**
- **Aprimorar os processos já existentes de auditoria e investigação por meio da coleta estruturada de logs e eventos, permitindo a análise detalhada de atividades fora dos padrões estabelecidos**.
- **Reduzir o risco de perda de dados sensíveis, por meio de políticas de criptografia em dispositivos de usuário final e mídias removíveis.**
- **Cumprir o art. 4º, §2º do Decreto nº 46.751/2019, e art. 5º, XVII, do Decreto nº 47.278/2020, que prescrevem a disponibilização de acesso a soluções de TIC aos demais órgãos da Administração Pública.**

15. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

15.1. Considerando que a solução a ser contratada será disponibilizada na modalidade SaaS (Software como Serviço), não são necessárias adaptações físicas, aquisições de infraestrutura ou contratações complementares para sua implantação.

15.2. Como providência administrativa, caberá à Administração garantir a disponibilidade dos recursos orçamentários necessários e formalizar a autorização para a contratação, conforme previsto na legislação vigente.

16. QUALIFICAÇÃO TÉCNICA

16.1. A presente contratação não prevê a exigência de atestado de qualificação técnica. Tal decisão visa ampliar a competitividade do certame, permitindo a participação de empresas que, embora não possuam experiência formalmente atestada na execução prévia de objetos idênticos, demonstrem plena capacidade de atendimento.

16.2. A mitigação de riscos quanto à aderência da solução às especificações do Termo de Referência será assegurada por dois mecanismos:

a) Realização de Prova de Conceito (POC), que consistirá em teste prático para verificação objetiva das funcionalidades e requisitos técnicos da solução antes da adjudicação ao vencedor; e

b) Exigência de comprovação de credenciamento, garantindo a idoneidade técnica e a autorização formal para fornecimento, suporte e atualização da solução, na forma do item 4.12.2.

16.3. Tais medidas permitem aferir, de forma concreta e prévia à contratação definitiva, a aptidão da solução proposta, mantendo a segurança técnica e a qualidade do objeto, em conformidade com os princípios da isonomia, competitividade e seleção da proposta mais vantajosa previstos na Lei nº 14.133/2021.

17. AMOSTRA, EXAME DE CONFORMIDADE E PROVA DE CONCEITO

17.1. Visando a comprovação dos aspectos e padrões mínimos de aceitabilidade, a LICITANTE classificada em primeiro lugar deverá cumprir todos os requisitos previstos na prova de conceito contida no Anexo III, deste documento (117796170).

17.2. Se a licitante convocada deixar de comparecer no dia designado para realização da prova de conceito sem justificativa aceita pelo pregoeiro, ou havendo incompatibilidade da solução com as especificações técnicas exigidas no edital, a proposta do licitante será recusada.

17.3. Se a Solução apresentada pelo primeiro classificado não for aceita, os integrantes técnicos da equipe de planejamento analisarão a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da Solução e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Anexo III.

17.4. A prova de conceito consistirá na apresentação do funcionamento do objeto, conforme especificações constantes do Anexo I - Especificações Técnicas do Objeto (117191792).

18. POSSIBILIDADE DE SUBCONTRATAÇÃO

18.1. Não será admitida subcontratação, tendo em vista a indivisibilidade técnica e operacional do objeto, cuja eficácia depende da integração plena entre os componentes da solução (plataforma, garantia técnica e capacitação), todos sob responsabilidade direta e contínua do mesmo fornecedor. A subcontratação parcial comprometeria o controle, a rastreabilidade e a segurança na execução, contrariando os princípios da eficiência e da mitigação de riscos que regem a presente contratação.

19. POSSIBILIDADE DE PARTICIPAÇÃO DE MICROEMPRESAS, PEQUENAS EMPRESAS E EMPRESÁRIOS INDIVIDUAIS

19.1. Não será aplicada reserva de cota para microempresas, empresas de pequeno porte ou empresários individuais, tendo em vista a natureza indivisível do objeto licitado. A subscrição de licenças de gerenciamento unificado de ativos é fornecida sob o modelo de subscrição integrada (SaaS), envolvendo plataforma, garantia técnica, atualizações contínuas, capacitação e monitoramento. Essa característica inviabiliza sua divisão em partes autônomas para adjudicação parcial a diferentes fornecedores, que admitem a não aplicação das regras de favorecimento a ME/EPP quando o objeto for tecnicamente indivisível ou exigir execução integrada e padronizada.

19.2. Ressalta-se ainda que não foram identificados, no levantamento de mercado, fornecedores de pequeno porte que, isoladamente, reúnam as condições técnicas, organizacionais e de certificação exigidas para a prestação integral do objeto com a robustez necessária, o que poderia implicar risco à segurança institucional e à continuidade dos serviços públicos críticos prestados pelo PRODERJ

20. POSSIBILIDADE DE PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS

20.1. Participação de Consórcios

20.1.1. É vedada a participação de pessoas jurídicas reunidas em consórcio.

20.1.2. A vedação à participação de interessadas que se apresentem constituídas em consórcio se justifica na medida em que nas licitações que visam à contratação de bens e serviços de TIC, existem no mercado empresas em quantidade e capacidade técnica suficientes para garantir um processo altamente competitivo e executar o objeto sem, necessariamente, se consorciar a outras empresas. A ausência de consórcio não trará prejuízos à competitividade do certame.

20.1.3. A importância de ser uma única empresa responsável pelo gerenciamento desses dados, evita a fragilidade das informações trazendo maior segurança dos processos.

20.1.4. Portanto, não será permitida a participação de empresas que estiverem reunidas em consórcio, qualquer que seja sua forma de constituição. Em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

20.2. Participação de Cooperativas

20.3. Não será admitida a participação de cooperativa de trabalho, qualquer que seja a sua forma de constituição, já que há vínculo de subordinação direta entre o empregado e a empresa contratada para a prestação dos serviços.

21. PRAZO DO CONTRATO E POSSIBILIDADE DE PRORROGAÇÃO

21.1. O prazo de vigência do Contrato-será de 36 (trinta e seis) meses, contado da divulgação no Portal Nacional de Contratações Públicas.

21.1.0.1. O prazo de vigência do Contrato poderá ser prorrogado, sucessivamente, até o máximo de 10 (dez) anos, na forma dos arts. 106 e 107 da Lei n° 14.133/2021, desde que observadas as condições previstas no Contrato, e mediante a celebração de termo aditivo.

22. LOCAL DE ENTREGA DOS BENS OU DA PRESTAÇÃO DO SERVIÇO

22.1. Por se tratar de subscrição de software na modalidade SaaS, a solução prevista será disponibilizada no endereço eletrônico fornecido pela CONTRATADA. A solução será mantida em infraestrutura de servidor da CONTRATADA, garantindo total disponibilidade para a CONTRATANTE durante a vigência do contrato. Para acesso ao ambiente virtual, assim como a instalação o treinamento deverão ser acordados em reunião de Kick-Off.

22.2. As demais especificações estão descritas no ANEXO I desde documento.

23. PRAZOS E CONDIÇÕES DE ENTREGA DOS SERVIÇOS

23.1. O prazo de entrega e instalação, será de até 45 (quarenta de cinco) dias corridos, após emissão da Autorização de Ordem de Serviço, que poderá ser emitida após a divulgação do contrato no Portal Nacional de Contratações Públicas, nos locais indicados pelo CONTRATANTE.

23.2. O prazo para a realização do treinamento, será de até 30 (trinta) dias corridos a contar da emissão da ordem de serviço, que poderá ser emitida após a divulgação do contrato no Portal Nacional de Compras Públicas (PNCP).

24. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E ACEITE DO OBJETO EXECUTADO (ANS)

24.1. Considerando a natureza dos serviços, cuja execução se dará por meio de Ordens de Serviço e o pagamento sob demanda, a avaliação da qualidade e o aceite do objeto ocorrerão mediante inspeção do fiscal técnico no recebimento provisório e definitivo, conforme o item "Regras para o recebimento provisório e definitivo", dispensando-se o monitoramento.

- **Finalidade:** Manter a qualidade da garantia do objeto.
- **Periodicidade:** Bimestral.
- **Início da medição:** A partir do 2º mês após a plena instalação e configuração da solução tecnológica (item 01).
- **Mecanismo de cálculo:** Somatório dos índices correspondentes aos eventos previstos nas alíneas "a, b, c, d, e" do subtópico 24.17 deste documento, verificados durante o período.

24.2. A contratada deverá cumprir prazos máximos para respostas aos acionamentos, de acordo com o nível de severidade de cada chamado, bem como os prazos de atendimento, conforme o quadro abaixo:

ATENDIMENTO			
Severidade	**Tempo máximo para início de atendimento**	**Tempo máximo para solução operacional**	**Grau de cumprimento**
CRÍTICO	Em até 30min	Em até 4 horas	95%
ALTA	Em até 1 hora	Em até 12 horas	95%
MÉDIA	Em até 2 horas	Em até 48h	90%
BAIXA	Em até 24 horas	Em até 72h	85%

24.3. A disponibilidade da ferramenta deve ser de 99,5% durante a vigência do contrato (cerca de 44 horas de indisponibilidade ao ano), caso o tempo de indisponibilidade ultrapasse o definido será considerada como severidade CRÍTICA.

24.4. O nível de severidade será informado pelo Contratante no momento da abertura do chamado, podendo ser reclassificado a critério do Contratante, caso em que ocorrerá início de nova contagem de prazo para o seu cumprimento.

24.5. O chamado não atendido no prazo estabelecido poderá ser reaberto, classificado no nível de severidade imediatamente superior, independentemente da aplicação das sanções aqui previstas.

24.6. O descumprimento deste acordo de nível de serviço, notadamente quanto ao cumprimento dos prazos, ensejará as sanções previstas no subtópico 2.17 deste documento.

24.7. Forma de atendimento: Os trabalhos deverão ser desenvolvidos por técnicos e consultores capacitados e certificados da CONTRATADA, através de instruções telefônicas, telepresenciais e presenciais para solução de problemas e operação dos componentes tecnológicos ou da intervenção remota através da Internet, utilizando para isto de ferramentas que garantam a confidencialidade das informações;

24.8. Tempo de resposta: Os atendimentos deverão ser respondidos e classificados em um prazo compatível com o nível de urgência especificado no momento da abertura do chamado ou identificação da anomalia e iminência de exploração, conforme descrito na tabela do subtópico

24.9. Tempo de solução: o tempo de solução de problemas dependerá de sua extensão, gravidade, disponibilidade e risco à disponibilidade ou integridade aos ativos da instituição. A CONTRATADA deverá fornecer uma estimativa de tempo para solução do problema dentro da primeira hora de atendimento.

24.10. Atendimento no local: Nos casos, classificados em grau de severidades Crítico/Alta, em que a intervenção remota não for efetiva, ou seja, após decorrido o prazo da estimativa de tempo fornecido para a solução do problema, a CONTRATADA deverá imediatamente, às suas custas, deslocar um técnico com o perfil necessário para atender ao problema em no máximo até 24 (vinte e quatro horas).

24.11. O técnico da CONTRATADA deverá apresentar, no ato do atendimento, credenciamento (crachá da empresa) e documento de identidade pessoal (RG), para efetuar qualquer serviço.

24.12. Informar à CONTRATANTE, quando da assinatura do contrato, as credenciais para acompanhamento de chamados junto ao fabricante oficial da solução. Este acompanhamento de chamados de suporte com o fabricante da solução deverá ser através da web ou via telefone 0800 do fabricante, sem ônus financeiros adicionais para o CONTRATANTE.

24.13. Caso sejam constatados problemas com a solução fornecida, tais como: mau funcionamento, erros de codificação, ou outras condições que impeçam/atrapalhem a execução das atividades dos usuários ou administradores da solução ofertada, que a CONTRATADA não consiga solucionar ou que extrapole seu campo de ação e conhecimento, deverá esta abrir chamado direto com o fabricante oficial da solução ofertada para tratamento do problema.

24.14. A Comissão de Fiscalização do Contrato a cada dois meses de apuração, deverá comunicar à Contratada o resultado da apuração.

24.15. A comunicação poderá ser feita pessoalmente, ou por meio eletrônico.

24.16. A CONTRATADA deverá enviar bimestralmente relatório resumido dos atendimentos eventualmente realizados no período.

24.17. **Sanções**

24.17.1. Ocorrerá aplicação de multas por motivo de descumprimento deste Acordo de Nível de Serviços, conforme os valores a seguir:

a) 0,10% do valor anual da solução a título de multa, por 10% de demandas categorizadas como "BAIXA" não atendidas no prazo, observados os limites quanto ao início do atendimento e solução operacional.

b) 0,20% do valor anual da solução a título de multa, por 5% de demandas categorizadas como “MÉDIA” não atendidas no prazo, dentro do período de apuração, observados os limites quanto ao início do atendimento e solução operacional.

c) 0,30% do valor anual da solução a título de multa, por 3% de demandas categorizadas como “ALTA” não atendidas no prazo, dentro do período de apuração, observados os limites quanto ao início do atendimento e solução operacional.

d) 0,50% do valor anual da solução a título de multa, por 1% de demandas categorizadas como “CRÍTICA” não atendidas no prazo, dentro do período de apuração, observados os limites quanto ao início do atendimento e solução operacional.

24.17.2. Os descontos relativos à redução por não cumprimento do nível de serviço não serão aplicados para demandas não rotineiras, no caso, por exemplo, de novas instalações;

24.17.3. Qualquer descumprimento do nível de serviço mínimo exigido poderá implicar a aplicação da legislação licitatória quanto à inexecução e à rescisão dos contratos;

24.17.4. Ficam resguardadas as demais sanções previstas em lei conforme o Edital.

25. CRITÉRIOS DE MEDIÇÃO, DE PAGAMENTO E FORMA DE REAJUSTAMENTO DO CONTRATO

25.1. **Reajuste de Preços**

25.1.1. Os preços contratados serão reajustados após o interregno de 1 (um) ano, mediante solicitação do CONTRATADO.

25.1.2. O interregno mínimo de 1 (um) ano para o primeiro reajuste será contado da data do orçamento estimado.

25.1.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir do fato gerador que deu ensejo ao último reajuste.

25.1.4. Os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do Índice de Custos de Tecnologia da Informação – ICTI, exclusivamente para as obrigações que se iniciem após a anualidade.

25.1.5. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, o CONTRATANTE pagará ao CONTRATADO a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

25.1.6. Fica o CONTRATADO obrigado a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer, sendo adotado na aferição final o índice definitivo.

25.1.7. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

25.1.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

25.1.9. O pedido de reajuste deverá ser formulado durante a vigência do contrato e antes de eventual prorrogação contratual, sob pena de preclusão.

25.1.10. Os efeitos financeiros do pedido de reajuste serão contados:

a) Da data-base prevista no contrato, desde que requerido o reajuste no prazo de 60 (sessenta) dias da data de publicação do índice ajustado contratualmente;

b) A partir da data do requerimento do CONTRATADO, caso o pedido seja formulado após o prazo fixado na alínea a, acima, o que não acarretará a alteração do marco para cômputo da anualidade do reajustamento, já adotado no edital e no contrato.

25.1.11. Caso, na data de eventual prorrogação contratual, ainda não tenha sido divulgado o índice de reajuste, deverá, a requerimento do CONTRATADO, ser inserida cláusula no termo aditivo de prorrogação para resguardar o direito futuro do CONTRATADO, a ser exercido tão logo se disponha dos valores reajustados, sob pena de preclusão.

25.1.12. A extinção do contrato não configurará óbice para o deferimento do reajuste solicitado tempestivamente, hipótese em que será concedido por meio de termo indenizatório.

25.1.13. O reajuste será realizado por apostilamento, se esta for a única alteração contratual a ser realizada.

25.1.14. O reajuste de preços não interfere no direito das partes de solicitar, a qualquer momento, a manutenção do equilíbrio econômico dos contratos com base no disposto no art. 124, inciso II, alínea "d", da Lei n.º 14.133/2021.

25.2. **De Pagamento**

25.2.1. O CONTRATANTE deverá pagar em parcela única e à vista o preço ao CONTRATADO, diretamente na conta-corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro, com direito de uso por 36 (trinta e seis) meses, a contar do recebimento definitivo.

25.2.2. No caso de o CONTRATADO estar estabelecido em localidade que não possua agência da instituição financeira contratada pelo Estado do Rio de Janeiro ou, caso verificada pelo CONTRATANTE a impossibilidade de o CONTRATADO, em razão de negativa expressa da instituição financeira contratada pelo Estado do Rio de Janeiro, abrir ou manter conta- corrente naquela instituição financeira, o pagamento poderá ser feito mediante crédito em conta-corrente de outra instituição financeira. Nesse caso, eventuais ônus financeiros e/ou contratuais adicionais serão suportados exclusivamente pelo CONTRATADO.

25.2.3. A emissão da Nota Fiscal ou Fatura será precedida do recebimento definitivo do objeto ou de cada parcela, mediante atestação, que não poderá ser realizada pelo ordenador de despesas, conforme disposto neste instrumento e/ou no Termo de Referência, bem ainda no artigo 140, II, alínea "b", da Lei nº 14.133/2021 e arts. 20 e 22, XXIII, do Decreto nº 48817/2023.

25.2.4. Quando houver glosa parcial do objeto, o CONTRATANTE deverá comunicar ao CONTRATADO para que emita Nota Fiscal ou Fatura com o valor exato dimensionado.

25.2.5. O CONTRATADO deverá encaminhar a Nota Fiscal ou Fatura para pagamento à CONTRATANTE para o endereço eletrônico a ser indicado.

25.2.6. Uma vez recebidos o documento mencionado no item 26.2.6, o órgão competente deverá verificar:

a) a manutenção das condições de habilitação exigidas pelo instrumento convocatório;

b) se o contratado foi penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o poder público mediante consulta aos cadastros oficiais do poder público existentes, observadas as abrangências de aplicação; e

c) por consulta ao SICAF, eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas apontadas ao Relatório de Ocorrências Impeditivas Indiretas.

25.2.7. Constatando-se a situação de irregularidade do CONTRATADO, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa e especifique provas que pretende produzir. O prazo poderá ser prorrogado uma vez, por igual período, a critério do CONTRATANTE.

25.2.8. Não havendo regularização ou sendo a defesa considerada improcedente, o CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do CONTRATADO, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

25.2.9. Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão do Contrato nos autos do processo administrativo correspondente, assegurada ao CONTRATADO a ampla defesa.

25.2.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso o CONTRATADO não regularize sua situação.

25.2.11. O pagamento será efetuado no prazo máximo de até 30 (trinta) dias, contados do recebimento da Nota Fiscal ou Fatura.

25.2.12. Havendo erro na apresentação da Nota Fiscal ou Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que o CONTRATADO providencie as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para o CONTRATANTE.

25.2.13. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

25.2.14. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

25.2.15. O CONTRATADO regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123/2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele Regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar nº 123/2006.

25.2.16. Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível ao CONTRATADO, sofrerão a incidência de atualização monetária e juros de mora pelo IPCA-E, calculado pro rata die, e aqueles pagos em prazo inferior ao estabelecido no instrumento convocatório serão feitos mediante desconto de 0,5% (um meio por cento) ao mês, calculado pro rata die.

25.2.17. O CONTRATADO deverá emitir a Nota Fiscal Eletrônica – NF-e, consoante o Protocolo ICMS nº 42/2009, com a redação conferida pelo Protocolo ICMS nº 85/2010, e caso seu estabelecimento esteja localizado no Estado do Rio de Janeiro, deverá observar a forma prescrita nas alíneas a, b, c, d e e, do §1º, do art. 2º da Resolução SEFAZ nº 971/2016.

25.2.18. Caso o CONTRATADO não esteja aplicando o regime de cotas na forma da Lei estadual nº 7.258, de 12 de abril de 2016, deste edital e do contrato, suspender-se-á o pagamento devido, até que seja sanada a irregularidade apontada pelo órgão de fiscalização do Contrato.

25.3. **Regime de execução**

25.3.1. O regime de execução é: EMPREITADA POR PREÇO UNITÁRIO.

26. **REGRAS PARA O RECEBIMENTO PROVISÓRIO E DEFINITIVO**

26.1. O objeto do contrato será recebido, na seguinte forma:

26.1.1. Subscrição de licenças, instalação e treinamento - (redação do art. 20, I, do Decreto 48.817/23):

a) provisoriamente, pelos fiscais dos contratos, mediante termo, no prazo de 15 (quinze) dias corridos após a entrega dos serviços, quando verificado o cumprimento das exigências de caráter técnico;

b) definitivamente, mediante parecer circunstanciado da comissão de fiscalização, após decorrido o prazo de 30 (trinta) dias corridos do recebimento provisório, para observação e vistoria, que comprove o exato cumprimento das obrigações contratuais;

26.1.2. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato ou termo de referência, podendo ser fixado pelo fiscal do contrato um prazo para a substituição do bem, ou o refazimento do serviço, às custas do contratado, sem prejuízo da aplicação das penalidades, sendo sempre necessário a motivação da recusa.

26.2. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos por este Decreto e pelo contrato.

26.3. Salvo disposição em contrário constante do edital, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

27. **CONDIÇÕES DE GARANTIA CONTRATUAL**

27.1. O Contrato conta com garantia de execução, nos moldes do artigo 96 da Lei nº 14.133/2021, correspondente a 3% (três por cento) de seu **valor anual**.

27.2. O referido percentual, resguardada a discricionariedade prevista no supracitado art. 96, caput e o teto estabelecido no caput do art. 98 do mesmo diploma legal, considera a natureza do objeto (bens e serviços), enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do órgão contratante em razão do volume de recursos financeiros envolvidos no certame, visando impedir a inexecução, mesmo que parcial do objeto e danos ao erário.

27.3. Caso o prazo de vigência do contrato seja inferior a um ano, a garantia aqui prevista será calculada sobre o valor total do Contrato.

27.4. O CONTRATADO poderá optar pelas seguintes modalidades de garantia:

a) caução em dinheiro ou em títulos da dívida pública;

b) seguro-garantia; e

c) fiança bancária.

d) título de capitalização custeado por pagamento único, com resgate pelo valor total.

27.5. Qualquer que seja a modalidade escolhida pelo CONTRATADO, a garantia assegurará o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações neste previstas;

b) multas moratórias, compensatórias e administrativas aplicadas pela Administração ao CONTRATADO; e

c) obrigações trabalhistas e previdenciárias de qualquer natureza, assim como as obrigações de regularidade perante o FGTS, não adimplidas pelo CONTRATADO, quando couber.

27.6. A garantia, qualquer que seja a modalidade escolhida, terá validade durante a vigência do Contrato e por mais 90 (noventa) dias após o término deste prazo de vigência.

27.7. Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o CONTRATADO ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.

27.8. Ressalvada a hipótese de seguro-garantia, em que deverá ser observado o prazo do item 27.9, o CONTRATADO apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do CONTRATANTE, contado da assinatura do Contrato, o comprovante de prestação de garantia, na forma do item 27.5.

27.9. Caso oferecida a modalidade de seguro-garantia, sua apresentação deve ocorrer em 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, e observar-se-ão as seguintes condições:

a) a apólice permanecerá em vigor mesmo que o CONTRATADO não pague o prêmio nas datas convencionadas;

b) a apólice deverá acompanhar as modificações referentes à vigência do Contrato principal, mediante a emissão do respectivo endosso pela seguradora;

c) será permitida a substituição da apólice na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 27.9; e

d) a apólice somente será aceita se contemplar todos os eventos indicados no item 27.5, observada a legislação que rege a matéria.

27.10. Em caso de oferecimento de títulos da dívida pública, estes devem ser emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

27.11. Caso a opção seja por fiança bancária, esta deverá ser emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil, e deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

27.12. Caso a opção seja por garantia em dinheiro, deverá ser efetuada em favor do CONTRATANTE, na conta-corrente da instituição financeira contratada pelo Estado, cujo valor será corrigido monetariamente e restituído ao CONTRATADO, na forma do item 27.21.

27.13. O CONTRATADO obriga-se a fazer a reposição, a suplementação ou a renovação da garantia, no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificado, no caso desta ser executada, total ou parcialmente, ou o Contrato for prorrogado ou tiver o seu valor alterado, assim como em qualquer outra situação que exija a manutenção da condição disposta no item 27.1 neste item.

27.14. A inobservância do prazo fixado para apresentação, reposição, suplementação ou renovação da garantia acarretará a aplicação de multa e/ou outras penalidades, na forma disposta no contrato.

27.15. O atraso superior a 25 (vinte e cinco) dias autoriza o CONTRATANTE a promover a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, com a aplicação das sanções cabíveis.

27.16. O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

27.17. O emitente da garantia ofertada pelo CONTRATADO deverá ser notificado pelo CONTRATANTE quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

27.18. O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções ao CONTRATADO.

27.19. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep n° 662, de 11 de abril de 2022.

27.20. Extinguir-se-á a garantia com a restituição da apólice, carta fiança, título da dívida pública ou autorização para a liberação da caução em dinheiro, atualizada monetariamente, acompanhada de declaração da CONTRATANTE, mediante termo circunstanciado, de que o CONTRATADO cumpriu todas as cláusulas do contrato.

27.21. A garantia somente será liberada ou restituída, após a fiel execução do Contrato ou pela sua extinção, por culpa exclusiva da Administração, ou quando assim convencionado, em se tratando de extinção consensual da contratação.

27.22. O CONTRATADO autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no edital e no Contrato.

27.23. No caso de inexecução total ou parcial do objeto, que acarrete a rescisão do Contrato, será automaticamente devida multa compensatória no valor de 5% do valor do Contrato, visando resguardar o órgão contratante em razão do volume de recursos financeiros envolvidos no certame.

28. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA

28.1. O presente documento, bem como os seus documentos anexos, consideraram a necessidade de contratação do objeto, os requisitos técnicos, legais, ambientais e os do próprio negócio, o mercado em que o objeto se encontra inserido, bem como todos os demais requisitos necessários para a caracterização e quantificação da demanda identificada, bem como o processo de escolha da solução que melhor se adequa à Instituição nesta oportunidade. Foram considerados ainda os requisitos ambientais e os aspectos legais, cabendo ressaltar que os riscos envolvidos são administráveis e os custos previstos são compatíveis e se caracterizam pela economicidade.

28.2. Desta forma, entende-se ser VIÁVEL a contratação em comento, e, visando dar início à implementação do objeto aqui delineado, recomenda-se a elaboração de Termo de Referência com base no presente documento e o encaminhamento para o setor competente para o prosseguimento do feito.

29. ANEXOS

29.1. Abaixo, estão listados os documentos anexos cujas disposições estão em plena concordância com este documento principal do qual correspondem a parte integrante e indissociável:

I - Especificações Técnicas do Objeto (117191792);

II - Mapa de Riscos (117192304);

III - Prova de Conceito (Teste de Conformidade) (117796170).

30. ASSINATURA DO RESPONSÁVEL

Daniel Luzente de Lima Diretor de Infraestrutura Tecnológica ID 4349885-0	**Élio Thomé de Souza Filho** Analista de Sistemas DIT ID 4347507-8	**Charles Monteiro Guimarães** Diretor de Patrimônio e Logística ID 4432892-3	**Marco Antônio de Andrade** Assessor Chefe da VPA ID. 4284601-3

Rio de Janeiro, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 30/10/2025, às 11:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Gerente**, em 30/10/2025, às 11:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 30/10/2025, às 12:01, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 30/10/2025, às 16:35, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **117192165** e o código CRC **5CA2E1B1**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Criado por praglb, versão 19 por praglb em 30/10/2025 10:54:02.

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice-Presidência de Tecnologia

ANEXO I DO ETP

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. ITEM 01 – SOLUÇÃO DE GESTÃO DE RELACIONAMENTO COM USUÁRIOS

1.1. Console/Gerenciamento

1.1.1. A plataforma deve possuir console web com acesso a todas as funcionalidades da solução, garantindo uma interface única para o gerenciamento dos endpoints.

1.1.2. O gerenciamento de todos os endpoints registrados deve ser possível através da console única, com visualização dos dispositivos em tempo real.

1.1.3. A plataforma deve implementar o modelo de Controle de Acesso Baseado em Perfis (RBAC), com a capacidade de atribuir permissões específicas a diferentes perfis para garantir a segregação adequada de funções.

1.1.3.1. A plataforma deve possuir perfis pré-configurados para as funções mais comuns, tais como operador, administrador e apenas leitura.

1.1.3.2. A plataforma deve permitir a criação de perfis customizados com controles granulares de permissões para cada funcionalidade.

1.1.4. Deve permitir integração com iDP (SAML 2.0) para autenticação e gerenciamento de identidade, oferecendo:

1.1.4.1. Importação e sincronização de usuários.

1.1.4.2. Autenticação de usuários e atribuição de papéis na console de gerenciamento com base em iDP.

1.1.4.3. Aplicação de políticas baseadas em grupos de iDP.

1.1.5. Deve permitir a instalação automática do software cliente em computadores de grupos predefinidos.

1.1.6. Deve permitir o uso de MFA (autenticação multifator) para maior segurança no acesso à plataforma.

1.1.7. Deve possuir logs de auditoria para fins de rastreabilidade das atividades realizadas na plataforma, com o recurso de exportação automatizada e segura dos logs para um repositório externo ou solução de SIEM.

1.1.8. Centralização de Visibilidade: Deve oferecer uma visão unificada e centralizada de todos os endpoints e sua saúde, incluindo visualizações em tempo real sobre status de conformidade, atualizações e alertas.

1.1.9. Deve fornecer dashboards padrões e personalizáveis que podem ser configurados para exibir informações relevantes sobre o estado dos endpoints, métricas de desempenho e alertas críticos.

1.1.10. Deve permitir a criação e gerenciamento de tarefas recorrentes e agendadas para manutenções e operações regulares, facilitando a automação de processos repetitivos.

1.1.11. Deve permitir a criação de grupos de endpoints estáticos e baseados em regras para a inserção dinâmica dos ativos, incluindo grupos baseados em atributos customizados.

1.1.12. A solução deve definir dinamicamente a criticidade do endpoint com base nos recursos/status do endpoint que o usuário determinar que melhor atendem às necessidades do negócio.

1.2. Arquitetura

1.2.1. A solução deve ser disponibilizada como uma oferta software como serviço "SaaS", capaz de gerenciar até 1.700 endpoints, sem necessidade de instalação de componentes no datacenter do cliente, VPN ou acesso via rede corporativa.

1.2.1.1. Esta solução SaaS pronta para uso deve ser hospedada fisicamente no Brasil.

1.2.2. A solução deve permitir fácil integração com soluções de segurança do tipo SIEM, com as seguintes funcionalidades:

1.2.2.1. Integração nativa por meio de socket com principais SIEMs de mercado, incluindo Splunk, ArcSight, QRadar e LogRythm

1.2.2.2. Integração customizada por meio de conexão HTTP e socket TCP

1.2.2.3. Definição de filtros e formato dos dados a serem enviados ao SIEM

1.2.2.4. Definição de recorrência do envio das informações ao SIEM

1.2.3. Deve ter funcionalidade para otimizar o consumo de banda na distribuição de pacotes em uma mesma LAN, com cache configurável.

1.2.4. Deve ter funcionalidade para limitar a comunicação com dispositivos em localidades com limitação de banda, permitindo a configuração de banda máxima, preservando a banda em situações de distribuição de pacotes.

1.2.5. Utilizar um único agente para todas as funcionalidades da solução, simplificando a implementação e o gerenciamento.

1.2.6. Permitir a segmentação de políticas de configuração, distribuição de softwares e patches por grupos de endpoints.

1.2.7. Integrar-se com ServiceNow para sincronização da base de dispositivos gerenciados com a base de itens de configuração do ServiceNow.

1.2.8. Permitir a exportação dos dados coletados, dados de telemetria, atributos, inventário de hardware e software via interface programável (API).

1.2.9. Desempenho de Escalabilidade: Deve possuir gerenciamento persistente para garantir o desempenho, estabilidade e segurança do ambiente, independente do número de ativos gerenciados.

1.2.10. Arquitetura de Distribuição de Conteúdo: Implementa uma arquitetura de distribuição de conteúdo descentralizada que utiliza ativos locais para otimizar a entrega de pacotes e minimizar o impacto na largura de banda.

1.2.11. A solução deve ser escalável para suportar a implementação global de mais de 1.700 dispositivos de endpoint em uma única interface de gerenciamento ou console

1.2.12. A solução deve suportar um ambiente que possua dispositivos com sobreposição de endereço IP.

1.2.13. A solução deve ser capaz de manter e rastrear um agente de endpoint conforme ele transita entre redes (por exemplo, onde os leases de DHCP expiram)

1.2.14. A solução deve ser capaz de transitar entre limites de NAT estático e PAT dinâmico.

1.2.15. A solução deve escalar sem a necessidade de servidores secundários de Distribuição/Retransmissão/Rollup dentro da LAN ou através da WAN.

1.2.16. A comunicação do cliente com a plataforma deve utilizar, no máximo, duas portas não padrão.

1.2.17. O tráfego entre o agente e a plataforma deve ser criptografado de ponta a ponta com protocolo TLS 1.3 ou superior.

1.2.18. Deve ser possível utilizar um proxy para a comunicação entre os clientes e a plataforma.

1.2.19. Deve realizar entrega de arquivos e pacotes de baixo impacto na rede através da rede sem o uso de servidores de distribuição secundários.

1.2.20. Usar um modelo de comunicação seguro de cliente para cliente em vez de um modelo de comunicação de servidor para cliente único para coletar dados e transmitir solicitações.

1.3. **3. Inventário e Descoberta**

1.3.1. Oferecer funcionalidade de descoberta para identificar novos dispositivos não gerenciados que se conectam à rede e sem agente instalado.

1.3.2. Coletar informações detalhadas sobre softwares instalados, incluindo nome, versão e fornecedor.

1.3.3. Permitir consultas em tempo real do inventário de hardware e software diretamente no(s) endpoint(s) através da console de administração.

1.3.4. Executar inventário de hardware e software de endpoints de forma recorrente e automatizada.

1.3.5. Apenas as diferenças (delta) são enviadas à base de dados central, minimizando a sobrecarga de rede.

1.3.6. Permitir a definição de atributos customizados para endpoints a partir de resultados de scripts ou valores em arquivos locais.

1.3.7. A solução deve categorizar todo o seu ambiente em minutos para apresentar uma reporte confiável dos softwares instalados nos dispositivos.

1.3.8. A solução deve fornecer inventários de gerenciamento de ativos de hardware (HWAM) e software (SWAM) e detalhes de gerenciamento de configuração (CSM) em todos os sistemas operacionais suportados em segundos a partir do início da solicitação.

1.3.9. Qualquer computador gerenciado pode identificar dispositivos não gerenciados na mesma sub-rede sem adicionar componentes de software adicionais nem abrir portas de rede adicionais.

1.4. **Medição de Uso de Software**

1.4.1. Medir o uso de softwares instalados com métricas de tempo e frequência de uso para Windows e MacOS.

1.4.2. Identificar padrões de uso de software, destacando as aplicações mais e menos utilizadas para Windows e MacOS, ajudando na otimização de licenças e na identificação de software não utilizado que pode ser desinstalado.

1.4.3. Gerar relatórios consolidados acessíveis via web, com opções de parametrização e filtragem para exibir quais ativos utilizam determinado software.

1.5. **Empacotamento e Distribuição de Software**

1.5.1. Deve permitir que um grupo de softwares seja atualizado de forma dinâmica conforme novas versões das aplicações que o compõem sejam lançadas, facilitando a manutenção de versões atualizadas sem a necessidade de modificar manualmente o grupo de software.

1.5.2. A solução deve vir com uma galeria de aplicativos que contenha, pelo menos, 300 aplicativos de mercado e os mantenha atualizados e disponíveis para uso sem exigir ações do usuário. Esta galeria deve incluir, no mínimo, navegadores web, aplicações de comunicação e conferência e aplicações de escritório.

1.5.3. Deve possuir suporte para empacotamento e distribuição de aplicativos desenvolvidos internamente.

1.5.4. Em caso de falha na instalação de software, deve ocorrer nova tentativa de forma automática, sem intervenção do usuário.

1.5.5. Deve suportar a verificação do resultado da distribuição de software com base em chaves de registro, arquivos de biblioteca e outros critérios.

1.5.6. Deve determinar o resultado da distribuição de software sem esperar pela varredura de inventário.

1.5.7. A solução deve permitir comparar a linha de base desejada com a linha de base atual e distribuir/remediar aplicações conforme necessário.

1.5.8. Deve permitir definir a sequência de instalação de pacotes de software.

1.5.9. Deve retomar automaticamente o envio de arquivos a partir do ponto de interrupção.

1.5.10. A solução deve verificar a integridade dos arquivos distribuídos.

1.5.11. Deve ser possível definir data/hora de expiração para tarefas de distribuição.

1.5.12. A solução deve permitir configurar a distribuição de forma síncrona ou escalonada automaticamente para o grupo alvo, incluindo a aplicação de patches.

1.5.13. Deve enviar notificações aos usuários de forma prévia para instalações/atualizações de software, com opção de postergar reboots.

1.5.14. A solução deve possuir uma loja de aplicativos para que os usuários possam instalar, atualizar e remover softwares autorizados pelo administrador para Windows e MacOS.

1.5.15. Deve ser possível agendar o deploy de software para ocorrer somente dentro de um intervalo de tempo programável.

1.5.16. Durante a distribuição de uma versão de software atualizada, deve remover versões anteriores.

1.5.17. A solução deve executar a distribuição de software condicionadas a atributos nativos ou customizados dos ativos.

1.5.18. Deve Implementar distribuição de conteúdo "peer-to-peer" ou tecnologia similar para reduzir a utilização de WAN.

1.5.19. A solução deve fornecer modelos para importação e implementação de software de terceiros.

1.5.20. A solução deve permitir que softwares não instalados pela plataforma sejam removidos dos dispositivos.

1.6. **Gerenciamento de Configurações Diversas**

1.6.1. A solução deve permitir explorar o diretório de arquivos e realizar o download e remoção de arquivos nos endpoints por meio da interface gráfica.

1.6.2. Deve permitir que o administrador da plataforma carregue scripts e pacotes para obter informações do endpoint (nome do computador, endereço IP, sistema operacional, usuário conectado, etc.) e também para alterar o estado do próprio endpoint (alterar uma chave de registro, interromper um serviço, etc.).

1.6.3. Deve executar scripts em dispositivos de forma agendada ou sob demanda.

1.7. **Patch Management**

1.7.1. Deve possuir repositório centralizado para download de patches disponibilizadas pelos fabricantes dos sistemas operacionais Windows e Linux sem a necessidade de empacotamento pelos administradores da solução.

1.7.2. Deve permitir a construção de baseline para assegurar que os ativos estejam sempre em conformidade com as políticas de patches definidas pelo administrador.

1.7.3. Deve possuir a capacidade de controlar a execução de reboot do dispositivo, com a possibilidade de configurar, para Windows e MacOS:

1.7.3.1. Um número máximo de vezes que o usuário pode adiar o reboot;

1.7.3.2. Reboots forçados depois de determinado número de adiamentos;

1.7.3.3. Reboot forçado por decurso de prazo.

1.7.4. Deve oferecer a capacidade de desinstalar um patch quando esta ação estiver habilitada pelo fabricante do sistema operacional Windows.

1.7.5. A solução deve contemplar a análise de confiabilidade de patches para sistema operacional Windows, em que informa a probabilidade de uma instalação de patch ser bem-sucedida com base na sua aplicação globalmente, incluindo taxa de desinstalação do patch.

1.7.6. A solução deve fornecer agendamento de patches e fluxos de trabalho personalizados e flexíveis para implementar um único patch em um grupo de computadores imediatamente ou executar tarefas mais complexas. Por exemplo, use conjuntos de regras avançadas e janelas de manutenção para fornecer grupos de patches em todo o ambiente em horários específicos.

1.7.7. A solução deve informar caso existam ativos que não atendam aos requisitos para a aplicação de patch, mostrando os motivos que podem impedir a aplicação do patch naqueles dispositivos.

1.7.8. A solução deve prover o status de implementação de qualquer patch, fornecendo feedback sobre sucessos, bem como falhas que exigem correção.

1.7.9. A solução deve fornecer históricos de patches para máquinas individuais, status de reinicialização do endpoint e links para artigos relevantes da base de conhecimento do fornecedor.

1.8. **Pontuações de Risco**

1.8.1. A solução deve calcular uma pontuação de risco de todo o ambiente de ativos com apresentação da evolução dessa pontuação ao longo do tempo

1.8.2. A solução deve permitir o cálculo da pontuação de risco de partes do ambiente, baseado em grupo de ativos, permitindo uma visualização isolada do risco de partes do ambiente.

1.8.3. A pontuação de risco deve levar em consideração as descobertas que elevam o potencial de risco, com base em informações como conformidade de configuração, criticidade dos dispositivos e uso de certificados expirados e cifras inseguras.

1.8.4. A avaliação de risco deve apresentar também informações operacionais que possam estar associados a um risco do ambiente, tais como necessidades de realização de reboot, uptime elevado e baixo espaço disponível em disco.

9. **Certificados Digitais**

1.8.5. Deve ser possível visualizar os certificados digitais utilizados no ambiente em dispositivos, permitindo a identificação rápida de:

1.8.5.1. Certificados digitais expirados ou perto da data de expiração

1.8.5.2. Utilização de chaves e algoritmos de criptografia considerados inseguros

1.8.5.3. Uso de certificados autoassinados e de autoridades certificadoras não autorizadas

1.8.5.4. Cifras criptográficas utilizadas em serviços ativos nos endpoints

1.8.6. A identificação dos certificados digitais do ambiente deve ser feita tanto com base nos certificados instalados nos dispositivos (arquivos e "certificate store" quanto nas portas de comunicação abertas (em escuta).

1.8.7. Para certificados nas portas de comunicação, deve ser possível visualizar o processo responsável pela porta de comunicação.

1.8.8. Deve ser possível exportar informações relativas aos certificados digitais do ambiente de forma periódica por e-mail

1.9. **Relatórios**

1.9.1. Deve disponibilizar relatórios pré-definidos com os principais usos da ferramenta, permitindo cloná-los para customização.

1.9.2. Deve permitir o uso de filtros para obtenção de subconjunto de dados.

1.9.3. Deve disponibilizar menus de criação e edição de relatórios com as seguintes funcionalidades:

1.9.3.1. Seleção do tipo ou item de configuração alvo do relatório;

1.9.3.2. Seleção de tabelas e campos relacionados somente ao tipo de item selecionado;

1.9.3.3. Classificação ascendente ou descendente para um ou mais campos selecionados;

1.9.3.4. Filtros para qualquer campo através de operadores igual, maior que, menor que, maior ou igual, diferente e caractere curinga;

1.9.3.5. Operadores booleanos E / OU ao usar múltiplos filtros;

1.9.3.6. Associação de múltiplas tabelas.

1.9.4. Deve permitir exportar os resultados de relatórios customizados em formatos diversos (Exemplo: JSON, HTML, CSV), possibilitando, também, o agendamento de execuções dos relatórios.

1.9.5. A solução deve permitir configurar gráficos para a visualização dos dados, sendo possível salvar as visualizações para compartilhamento.

1.10. **Experiência do Usuário**

1.10.1. Permitir customizar, agendar e definir público-alvo de surveys, com oferta direta na área de trabalho do usuário, sem a necessidade de componentes e integrações adicionais, facilitando a captura da "voz do cliente " em relação aos serviços de TI ofertados para Windows e MacOS.

1.10.2. Deve identificar, coletar e agregar dados/telemetria de usuário, aplicações e dispositivos, para exibir uma visão de Digital Employee Experience, para sistemas operacionais Windows e MacOS.

1.10.3. A solução deve coletar feedback em tempo real dos usuários sobre o desempenho e a experiência com os dispositivos e serviços, permitindo tomada de decisão baseada em dados.

1.10.4. Permite a criação de ações automatizadas com base na ocorrência de situações que possam afetar o desempenho do usuário com notificação e apresentação de ação a ser executada pela plataforma para remediação.

1.10.5. Deve ser possível criar notificações a serem enviadas aos usuários, possibilitando o informe de ocorrências, lembretes ou informações importantes.

1.10.5.1. Deve suportar a customização da aparência da janela de notificação aos usuários;

1.10.5.2. Deve permitir o agendamento do envio das notificações;

1.10.5.3. Deve permitir o envio das notificações a determinados grupos de dispositivos

1.11. **Desempenho**

1.11.1. Possuir capacidade para cálculo automático de "Scores" para mensuração da saúde dos endpoints para Windows, Linux e MacOS.

1.11.2. Possuir capacidade para identificar anomalias, mensurar o nível de utilização dos dispositivos, suas aplicações e realizar análise de causa raiz com base em sua própria telemetria.

1.11.3. Coletar e armazenar dados de consumo de CPU e de memória por aplicação em cada um dos endpoints gerenciados.

1.12. **Agente**

1.12.1. A solução deve executar todos os requisitos usando um único agente unificado

1.12.2. O agente de endpoint deve ser oculto ao usuário final

1.12.3. A solução deve oferecer suporte a clientes em ambiente local

1.12.4. A solução deve oferecer suporte a clientes em ambientes de nuvem multilocatários (por exemplo, AWS, Azure)

1.12.5. O agente de endpoint deve ser fornecido em um formato de implantação comum compatível com ferramentas de empacotamento padrão para automatizar a implantação

1.12.6. Suporte de agentes para os seguintes Sistemas Operacionais:

1.12.6.1. Windows 7 SP1 e posterior.

1.12.6.2. Windows 2008 R2, SP1 e posterior.

1.12.6.3. SUSE Linux 12.x e posterior.

1.12.6.4. Oracle Linux 5.x e posterior.

1.12.6.5. Red Hat Enterprise Linux 5.x e posterior.

1.12.6.6. CentOS Linux 5.x e posterior.

1.12.6.7. Debian 8 e posterior.

1.12.6.8. macOS 10.14 e posterior.

1.12.6.9. Ubuntu 14.04 LTS e posterior.

1.12.6.10. IBM AIX 7.1 e posterior.

1.12.6.11. Solaris 10 U8 e posterior.

1.12.7. O agente deve se comunicar com a console de gerenciamento e relatórios quando não estiver conectado à rede corporativa (por exemplo, ao trabalhar remotamente ou conectado à Internet)

1.13. **Automação**

1.13.1. A solução deve incluir recursos de automação sem código que permitem a configuração de múltiplas ações em sequência, incluindo controles e notificações na sequência de automação.

1.13.2. A solução deve permitir que o usuário configure seus próprios playbooks de automação customizados.

1.13.3. A solução deve permitir que o usuário crie o máximo de etapas possível dentro de um playbook e tais etapas devem fornecer funcionalidades para executar ações, coletar entrada/confirmação do usuário, exibir notificações ao usuário final, verificar condições, e aguardar por um tempo determinado.

1.13.4. O usuário deve ser capaz de automatizar a execução do playbook com base em cronograma, eventos, e condições.

1.13.5. O usuário deve ser capaz de ver o status de execução de qualquer playbook que tenha sido executado e deve ser capaz de rastrear o status de execução de cada etapa dentro do playbook.

1.13.6. Deve ser possível enviar notificações de e-mail referentes às execuções dos playbooks de automação.

2. **REUNIÃO DE KICK-OFF**

2.0.1. A CONTRATADA deve realizar, antes do início da implantação da solução, uma reunião inicial de projeto (kick-off) com a CONTRATANTE.

2.0.2. A CONTRATANTE deverá acionar as suas áreas que serão responsáveis pela Segurança da Informação, Infraestrutura, Gestão e Fiscalização do Contrato, para em conjunto com a CONTRATADA para definirem o local de implantação, preparação do ambiente, instalação e configuração da solução.

2.0.3. Após a reunião de kick-off deve ser produzida uma ata e assinada por todos os participantes da CONTRATADA e da CONTRATANTE presentes, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, discriminação da EQUIPE do projeto com perfis e quantitativos mínimos, relatório de controle e tratamento de riscos do projeto e demais artefatos que se façam necessários no entendimento da Contratada.

2.0.4. Na reunião inicial, serão abordados alguns pontos e informações citadas a seguir, mas não se limitando a:

a) Apresentação das equipes envolvidas, com definição dos responsáveis técnicos e gerenciais de ambas as partes;

b) Validação do escopo detalhado dos produtos e serviços contratados, com ênfase nas etapas de instalação, configuração, suporte técnico e treinamentos;

c) Definição e validação do cronograma de execução, com marcos de entregas, prazos intermediários e critérios para aceite de cada fase;

d) Estabelecimento dos canais formais de comunicação e reporte, assim como dos instrumentos de acompanhamento e controle da execução contratual (relatórios, reuniões periódicas, ferramentas de gestão, etc.);

e) Levantamento e verificação de pré-requisitos técnicos e operacionais para o início da execução, incluindo:

- Disponibilidade e configuração dos ambientes (produção e testes);
- Necessidade de provisionamento de acessos, credenciais e perfis de usuários;
- Infraestrutura mínima necessária (rede, banco de dados, servidores, etc.);
- Integrações com sistemas legados eventualmente envolvidos;
- Apoio necessário por parte da equipe interna da contratante; e

f) Dinâmica de capacitação;

Rio de Janeiro, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 30/10/2025, às 11:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Gerente**, em 30/10/2025, às 11:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 30/10/2025, às 12:01, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 30/10/2025, às 16:35, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **117191792** e o código CRC **39A9A6B2**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Criado por praglb, versão 5 por praglb em 30/10/2025 11:00:05.

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice-Presidência de Tecnologia

ANEXO II DO ETP

MAPA DE RISCOS

1. OBJETO

Contratação de empresa especializada fornecimento de Subscrição de licenças de gerenciamento unificado de ativos baseada em nuvem, com garantia de 36 meses, o serviço de instalação da solução e o treinamento especializado.

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

No escopo da presente contratação, foram identificados os riscos inerentes ao negócio, os passíveis de comprometer o êxito do processo de contratação e os referentes à gestão contratual.

Cada risco identificado foi enquadrado conforme seu tipo (infraestrutura, segurança ou organizacional), considerando-se a probabilidade de ocorrência dos eventos, os possíveis danos potenciais em caso de acontecimentos, as possíveis ações preventivas e de contingências, bem como a identificação de responsáveis por ação. Para tanto, tais riscos foram classificados a partir da atribuição de valores aos níveis de probabilidade (P) e impacto (I), conforme tabela abaixo:

Escala Qualitativa de Classificação	
Classificação	**Valor**
Baixo	5
Médio	10
Alto	15

Em seguida, o produto obtido da relação entre a probabilidade e o impacto resultou na elaboração da Matriz Probabilidade x Impacto, instrumento responsável pela definição dos critérios quantitativos de classificação do nível de risco, a fim de direcionar as ações relacionadas aos riscos durante a fase de planejamento e gestão do contrato.

Probabilidade (P)	15	**75**	**150**	**225**
	10	**50**	**100**	**150**

	5	**25**	**50**	**75**
Impacto (I)		5	10	15

Caso o risco se enquadre na região verde, seu nível de risco é entendido como baixo, logo, admite-se sua aceitação ou adoção das medidas preventivas, por meio do uso de controles de segurança. Se estiver na região amarela, entende-se como médio; e se estiver na região vermelha, entende-se como nível de risco alto. Nos casos de riscos classificados como médio e alto, deve-se adotar obrigatoriamente os controles de segurança previstos.

Uma vez definidos os riscos e seus níveis, indicou-se a resposta de ação correspondente a cada um deles, de acordo com o quadro abaixo:

Respostas aos riscos	
Evitar	Eliminar o risco, evitando-o totalmente.
Mitigar	Reduzir a probabilidade e/ou o impacto do risco, ação realizada independente do risco ocorrer ou não.
Transferir	Passar o custo da consequência para um terceiro.
Aceitação Ativa	Criar um plano de contingência para ser acionado, caso o risco ocorra.
Aceitação Passiva	Não tomar nenhuma ação preventiva, lidando com o problema apenas caso o risco ocorra.

A partir do percurso metodológico descrito, foram identificados os seguintes riscos:

Tabela de relação de riscos identificados						
Id	**Risco**	**Tipo de Risco**	**Probabilidade**	**Impacto**	**Nível de Risco (P X I)**	**Respostas aos Riscos**
R1	Dependência tecnológica a ser estabelecida entre a contratante e contratada	Risco de Infraestrutura	10	10	100	Mitigar/ Aceitação Ativa
R2	Especificação incorreta ou incompleta da solução desejada	Risco de Infraestrutura	5	15	75	Mitigar/ Aceitação Ativa
R3	Interrupção do serviço	Risco de Infraestrutura	5	15	75	Mitigar/ Aceitação Ativa

R4	Atraso ou suspensão no processo licitatório em face de impugnações	Risco organizacional	5	15	75	Evitar/ Aceitação Ativa
R5	Ausência de recursos orçamentários ou financeiros	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R6	Descumprimento das cláusulas contratuais pela contratada	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R7	Descumprimento dos níveis de serviço estabelecidos	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R8	**A empresa contratada não ter capacidade de entregar o objeto**	Risco organizacional	5	15	75	Mitigar/ Aceitação Ativa
R9	**Dificuldade na fiscalização do contrato**	Risco organizacional	10	15	150	Mitigar/ Aceitação Ativa

3. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

3.1. Riscos de Infraestrutura

Risco 1	**Risco:**		Dependência tecnológica a ser estabelecida entre a Contratante e a Contratada
	Probabilidade:		Média
	Impacto:		Médio
	Dano 1:		Dependência excessiva da solução.
	Dano 2:		Desuso da solução após término de contrato.
	Id	**Ação Preventiva**	**Responsável**
	1	Buscar e manter conhecimento sobre solução simular aos produtos contratados	Área Técnica
	2	Manter o conhecimento do serviço e dos processos de execução sob controle da Contratante, de modo a reduzir o risco de dependência em relação ao fornecedor.	Equipe de Fiscalização do Contrato

	3	Promover o monitoramento contínuo da execução contratual, por meio de registro histórico, com o objetivo de garantir a continuidade dos serviços e evitar sua interrupção de forma não programada.	Equipe de Fiscalização do Contrato
	Id	**Ação de Contingência**	**Responsável**
	1	Realização de novo procedimento licitatório com antecedência ante a impossibilidade de prorrogação do contrato atual.	Equipe de Licitação

Risco 2	**Risco:**	Especificação incorreta ou incompleta da solução desejada	
	Probabilidade:	Baixo	
	Impacto:	Alto	
	Dano 1:	Deficiência na execução dos serviços.	
	Dano 2:	Não atingimento completo dos resultados elencados nos artefatos de planejamento da contratação.	
	Id	**Ação Preventiva**	**Responsável**
	1	Garantir que o Estudo Técnico Preliminar seja elaborado de forma adequada, englobando todo o escopo necessário ao atingimento dos resultados esperados.	Equipe de Planejamento da Contratação
	2	Revisar cuidadosamente o Termo de Referência quando o objeto possuir especificações técnicas ou condições de fornecimento específicos.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Retornar à análise de viabilidade da contratação e verificar a solução que melhor atenda às necessidades de negócio.	Área Técnica e Área de Negócio

Risco 3	**Risco:**	Interrupção do serviço
	Probabilidade:	Baixa
	Impacto:	Alto
	Dano 1:	Interrupção da prestação dos serviços de atualização e da garantia, podendo gerar falhas de segurança e impossibilidade de atualização das versões.

	Id	**Ação Preventiva**	**Responsável**
	1	Garantir que o Termo de Referência defina a aplicação de penalidades proporcionais em caso de interrupção abrupta dos serviços.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar as sanções administrativas previstas no Contrato.	Comissão de Fiscalização do Contrato
	2	Verificar junto à empresa as condições para o restabelecimento da prestação do serviço.	Comissão de Fiscalização do Contrato
	3	Iniciar elaboração de novo procedimento licitatório, caso haja rescisão contratual.	Equipe de Licitação

3.2. Riscos Organizacionais

Risco 4	**Risco:**		Atraso ou suspensão no processo licitatório em face de impugnações e recursos
	Probabilidade:		Alta
	Impacto:		Alto
	Dano 1:		Demora ou impedimento da contratação.
	Id	**Ação Preventiva**	**Responsável**
	1	Verificar e avaliar os pontos que levam à licitação deserta/frustrada, bem como impugnações e recursos em contratações similares, para evitar que estas causas sejam reproduzidas no procedimento licitatório.	Equipe de Planejamento da Contratação
	2	Dar celeridade ao processo licitatório, dentro das condições impostas no edital.	Equipe de Licitação
	3	Estabelecer condições técnico-administrativas no Termo de Referência que não restrinjam a competitividade do certame.	Área Técnica
	4	Revisar os artefatos de planejamento da contratação.	Equipe de Planejamento da Contratação

	Id	**Ação de Contingência**	**Responsável**
	2	Alteração de condições técnico-administrativas do Termo de Referência, a fim de que possam permitir o andamento do processo licitatório, desde que não desnaturem o objeto.	Equipe de Planejamento da Contratação

Risco 5	**Risco:**	Ausência de recursos orçamentários ou financeiros	
	Probabilidade:	Baixa	
	Impacto:	Alto	
	Dano 1:	Atraso e/ou interrupção do processo de contratação.	
	Dano 2:	Perda do acesso das subscrições.	
	Dano 3:	Perda da possibilidade de atualizar as licenças perpétuas pela não realização de pagamento em prazo superior a 90 (noventa) dias.	
	Id	**Ação Preventiva**	**Responsável**
	1	Verificar o alinhamento estratégico da contratação ao PEDTIC e aos documentos de planejamento do órgão (PAC).	Equipe de Planejamento da Contratação
	2	Reservar os recursos orçamentários.	Ordenador de Despesas
	3	Expor à Alta Administração, bem como ao Ordenador de Despesa, a importância e relevância da contratação.	Área de Negócio
	Id	**Ação de Contingência**	**Responsável**
	1	Verificar possibilidade de operação de crédito para execução da despesa.	Ordenador de Despesas
	2	Realizar novo procedimento licitatório para contratação do Objeto	Equipe de Licitação

Risco 6	**Risco:**	Descumprimento das cláusulas contratuais pela Contratada
	Probabilidade:	Baixa
	Impacto:	Alto

	Dano 1:		Não entrega dos serviços contratados.
	Dano 2:		Atraso no início da execução dos serviços.
	Dano 3:		Qualidade insatisfatória dos serviços prestados.
	Dano 4:		Descontinuidade dos serviços.
	Dano 5:		Falta de efetividade da contratação.
	Id	**Ação Preventiva**	**Responsável**
	1	Acompanhar a execução dos serviços, aferindo se os requisitos previstos pelo instrumento contratual e pelo Termo de Referência estão sendo cumpridos de acordo com os níveis de qualidade estabelecidos.	Comissão de Acompanhamento e Fiscalização do Contrato
	2	Designar Comissão de Acompanhamento e Fiscalização do Contrato composta por servidores capazes de fiscalizar efetivamente o contrato.	Alta Gestão
	Id	**Ação de Contingência**	**Responsável**
	1	Notificar formalmente a Contratada quando cláusulas do contrato forem descumpridas.	Comissão de Acompanhamento e Fiscalização do contrato
	2	Aplicar de multa moratória e as penalidades previstas no contrato, de forma a coibir a reincidência de descumprimentos contratuais.	Comissão de Acompanhamento e Fiscalização do contrato
	3	Rescindir o contrato unilateralmente e iniciar novo processo de contratação, utilizando os artefatos de planejamento produzidos, com as atualizações baseadas na experiência adquirida no processo de gestão e fiscalização.	Comissão de Acompanhamento e Fiscalização do contrato / Alta Gestão / Equipe de Planejamento da Contratação

Risco 7	**Risco:**	Descumprimento dos níveis de serviço estabelecidos
	Probabilidade:	Baixa
	Impacto:	Alto
	Dano 1:	Impacto negativo sobre a qualidade dos serviços prestados, não atendendo aos requisitos estabelecidos no Termo de Referência.

	Id	**Ação Preventiva**	**Responsável**
	1	Atribuir multa moratória e sanções razoáveis no Termo de Referência que disciplinem a continuidade dos serviços de forma satisfatória.	Comissão de Acompanhamento e Fiscalização do contrato
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar as sanções administrativas, conforme previstas no Termo de Referência e no Contrato.	Comissão de Acompanhamento e Fiscalização do contrato

Risco 8	**Risco:**		**A empresa contratada não ter capacidade de entregar o objeto.**
	Probabilidade:		Baixa
	Impacto:		Alto
	Dano 1:		Fracasso do processo licitatório Não alcançar os objetivos propostos Perdas financeiras causadas pela utilização de tecnologias mais caras durante um período mais prologando
	Id	**Ação Preventiva**	**Responsável**
	1	O termo de referência deverá solicitar atestado de capacidade técnica capaz de determinar se a empresa vencedora do certame realmente está capacitada a fornecer o objeto contratado.	Equipe de Planejamento da Contratação
	Id	**Ação de Contingência**	**Responsável**
	1	Aplicar punições cabíveis a CONTRATADA que não cumprir os termos estabelecidos no termo de referência e no contrato. Tomar ações jurídicas cabíveis caso a empresa não comprove que os atestados entregues são verdadeiros.	Área técnica e jurídica.

Risco 9	**Risco:**	**Dificuldade na fiscalização do contrato**
	Probabilidade:	Médio

Impacto:		Alto
Dano 1:		Não alcançar os objetivos da contratação Realizar pagamentos não condizentes com os serviços prestados.
Id	**Ação Preventiva**	**Responsável**
1	O termo de referência deverá estabelecer um instrumento de medição de resultados eficiente, capaz de estabelecer critérios objetivos na medição e avaliação dos serviços prestados.	Equipe de Planejamento da Contratação
Id	**Ação de Contingência**	**Responsável**
1	Aplicar glosas e sanções previstas no IMR (Instrumento de medição de resultados)	Comissão de Acompanhamento e Fiscalização do contrato

Rio de Janeiro, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 30/10/2025, às 11:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Gerente**, em 30/10/2025, às 11:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 30/10/2025, às 12:01, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 30/10/2025, às 16:35, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **117192304** e o código CRC **DDC51B47**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Criado por praglb, versão 4 por praglb em 30/10/2025 10:48:29.

Governo do Estado do Rio de Janeiro

Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Vice Presidência de Tecnologia

ANEXO III DO ETP

EXAME DE CONFORMIDADE

1. ROTEIRO PARA TESTE DE CONFORMIDADE

1.1. O licitante classificado em primeiro lugar, deverá proceder conforme disciplinado neste Anexo - Exame de Conformidade, sob pena de não aceitação da proposta.

1.2. Exame será realizado em um dos seguintes endereços do PRODERJ, conforme designação da Administração:

- Rua São Francisco Xavier, 524 – 2º andar, bloco "F" – Maracanã – Rio de Janeiro/RJ – CEP 20550-013 (Data Center – UERJ);
- Rua Carmo Neto, s/nº – Cidade Nova – Rio de Janeiro/RJ – CEP 20210-051 (Data Center – CICC);
- Rua da Conceição, 69 – 24º e 25º andares – Centro – Rio de Janeiro/RJ – CEP 20051-011 (Sede – PRODERJ).

1.3. Por meio de mensagem no sistema, será divulgada a data e horário de realização do procedimento de exame, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

1.4. Os resultados dos exames serão divulgados por meio de mensagem no sistema.

1.5. No caso de não observância ao procedimento definido no Termo de Referência quanto ao exame de conformidade, sem justificativa aceita pelo Pregoeiro, ou se constatando o não atendimento das especificações previstas no Edital, a proposta do licitante será recusada.

1.6. Se o resultado do exame de conformidade realizado pelo primeiro classificado for de desconformidade, o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com os exames na forma deste item 1 e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência e neste Anexo.

1.7. O licitante classificado em primeiro lugar deverá realizar exame de conformidade, como disciplinado neste anexo - Exame de Conformidade, no prazo de 10 (dez) dias corridos a contar da solicitação do pregoeiro via chat do SIGA-RJ. O prazo poderá ser prorrogado por 10 (dez) dias corridos mediante requisição fundamentada do licitante, sob pena de não aceitação da proposta.

1.8. Os licitantes que tenham participado da etapa competitiva e desejem acompanhar a realização do Exame de Conformidade, deverão encaminhar e-mail endereçado à Comissão de Pregão (cdl@proderj.rj.gov.br). Serão aceitos pedidos de acompanhamento recebidos até as 16:00h do dia que antecede a data de realização do Exame de Conformidade. No e-mail deverão constar: dados da empresa interessada (nome, CNPJ e contato) e de seu representante (RG, CPF e contato) para o devido credenciamento.

1.9. O Exame de Conformidade será realizado preferencialmente no PRODERJ no endereço: Rua da Conceição n° 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP: 20051-011.

1.10. O Exame de Conformidade será realizado, preferencialmente, em horário comercial entre 09h às 13h e 14h às 18h (horário de Brasília).

1.11. O licitante classificado em primeiro lugar na fase de lances deverá entregar em conjunto com a documentação de habilitação e proposta comercial, os manuais técnicos da solução de gerenciamento unificado de ativos ofertada, que comprovem os requisitos técnicos funcionais previstos no Anexo I - Especificações Técnicas. Deverá apresentar planilha ponto a ponto de verificação de atendimento às especificações técnicas, a fim de facilitar a verificação da adequação da solução proposta às características técnicas obrigatórias constantes neste Anexo, contendo as indicações precisas, na documentação da solução, que comprovem todas as características técnicas exigidas.

1.12. Somente serão aceitos para comprovação das características técnicas documentos originais do fabricante (datasheets, sites ou documentação oficial do fabricante) específicos à solução ofertada, escritos em português ou inglês, não sendo admitidas montagens ou adaptações, totais ou parciais, sobre o texto deste documento.

1.13. A equipe técnica do PRODERJ analisará os manuais técnicos funcionais, verificando se os requisitos previstos no Termo de Referência, no Anexo I de Especificações Técnicas e no roteiro constante neste Anexo, são atendidos em sua totalidade pela solução. Caso a licitante melhor classificada logre êxito na fase de documentação técnica será convidada a realizar o Exame de Conformidade, conforme abaixo:

a) O Exame de Conformidade não deverá ter custo adicional ao CONTRATANTE;

c) As atividades serão realizadas em data a ser oportunamente publicada aos LICITANTES pelo(a) pregoeiro(a);

1.14. O prazo máximo para a conclusão de todas as etapas previstas no Exame de Conformidade será de 5 (cinco) dias úteis a partir da data de informada pelo(a) pregoeiro(a);

1.15. O Exame de Conformidade será acompanhado por equipe técnica a ser indicada pela CONTRATANTE;

1.16. A CONTRATANTE disponibilizará até 5 (cinco) ativos/endpoints (Windows e Linux) para serem incluídos na solução de gerenciamento unificado de ativos ofertada, a ser executado durante o exame de conformidade;

1.17. A CONTRATANTE fará a avaliação para garantir a plena execução de todas as atividades relativas ao Exame de Conformidade, e ainda:

a) Emitirá o “Relatório de conclusão da avaliação técnica”;

c) Emitirá o termo de aceite definitivo ou de recusa da solução, para fins de continuidade do procedimento licitatório, no prazo de 05 (cinco) dias após o encerramento do Exame de Conformidade.

1.18. No dia da realização do Exame de Conformidade um representante credenciado da licitante deverá estar presente para sanar quaisquer dúvidas ou divergências levantadas pela equipe técnica;

1.19. Para confirmação das especificações funcionais (durante a realização do Exame de Conformidade), não será autorizado o uso de slides ou vídeos.

1.20. Não será autorizado modificar ou gravar códigos em qualquer mídia durante e após a realização do Exame de Conformidade.

1.21. A violação a qualquer uma das regras estabelecidas desclassifica o licitante.

1.22. Quaisquer dificuldades que impeçam a continuidade dos trabalhos ou que provoquem atividades adicionais para realização do Exame de Conformidade (pelos processos internos dos entes públicos), não terão seu tempo contabilizado para o prazo do Exame de Conformidade, não se admitindo que sejam considerados como prejuízo ao licitante durante a avaliação.

1.23. Caso o licitante não compareça na data e horário designados pelo pregoeiro ou, se não atendidos por qualquer motivo, os requisitos descritos neste documento, o licitante será desclassificado.

1.24. Concluído o Exame de Conformidade a equipe técnica do PRODERJ considerará apto o sistema que atender a todos os requisitos relacionados no roteiro estabelecido neste documento, onde cada item deverá ser preenchido, assinalando-se "atende" ou "não atende".

1.25. O relatório final de avaliação será encaminhado ao pregoeiro e publicado no sistema SIGA.

1.26. Será desclassificado o licitante que, convocado para o Exame de Conformidade não demonstrar a compatibilidade do seu produto com as especificações técnicas exigidas ou não comparecer no dia marcado sob qualquer pretexto.

1.27. A desclassificação dará início ao processo de qualificação do próximo qualificado na fase de preços, resguardadas todas as condições e prazos previstos neste tópico;

1.28. O licitante desclassificado no Exame de Conformidade não terá direito a qualquer indenização.

1.29. Todos os prazos estabelecidos neste tópico serão contados em “dias corridos”.

1.30. O Exame de Conformidade será composto pela homologação das funcionalidades, características e demais evidências acerca da solução de gerenciamento unificado de ativos, de forma a permitir a validação dos requisitos técnicos do edital, especialmente aqueles que não podem ser verificados apenas por análise documental, garantindo:

- Coleta e atualização em tempo real do inventário de hardware e software;
- Descoberta de ativos não gerenciados;
- Distribuição de software com controle de banda e resiliência;
- Segurança e criptografia nas comunicações;
- Avaliação de risco e experiência do usuário.

1.31. O Exame será realizado pela LICITANTE, seguindo o roteiro estabelecido abaixo, que não contempla todas os requisitos a serem verificados e, portanto, a aprovação de todos os itens do roteiro não exime a licitante de ter de comprovar a aderência da solução a todos os requisitos estabelecidos no Termo de Referência, especialmente o Anexo I de Especificações Técnicas.

Roteiro do Exame de Conformidade

SOLUÇÃO DE GERENCIAMENTO UNIFICADO DE ATIVOS			
Descoberta e Inventário:	**APROVADO**		**RESULTADO E OBSERVAÇÃO**
	SIM	**NÃO**	
Instalar o agente em 5 endpoints e conectar à console SaaS.			
A solução tem a capacidade de descobrir dispositivos não autorizados			
Modificar uma aplicação instalada em um endpoint e verificar atualização de inventário.			
Criar atributo customizado via script local e exibir na console.			
Demonstrar que a solução é capaz de coletar o inventário de hardware e software nos dispositivos onde o agente está instalado			
Demonstrar que a solução é capaz de consultar informações de inventário, status, item de configuração em tempo real			
Demonstrar que a solução é capaz de rastrear a efetiva utilização de aplicativos instalados nas estações de trabalho			
Integração e Segurança da Arquitetura	**APROVADO**		**RESULTADO E OBSERVAÇÃO**
	SIM	**NÃO**	
Confirmar acesso via console web sem VPN ou conexão à rede corporativa.			
Verificar comunicação agente–plataforma utilizando **TLS 1.3 ou superior**.			
Simular mudança de rede (endereço IP ou NAT).			
Gestão de Patches	**APROVADO**		

	SIM	**NÃO**	**RESULTADO E OBSERVAÇÃO**
Realizar varredura automática de patches pendentes.			
Implantar patch em grupo de endpoints com janelas diferentes.			
Avaliar confiabilidade do patch (probabilidade de sucesso).			
Demonstrar que a solução é capaz de aplicar patches em sistemas Windows			
Demonstrar que a solução é capaz de aplicar patches em sistemas Linux			
Distribuição e Empacotamento de Software	**APROVADO**		**RESULTADO E OBSERVAÇÃO**
	SIM	**NÃO**	
Implantar um pacote de software em 3 endpoints simultaneamente.			
Interromper a rede durante o deploy e restabelecer após 1 minuto.			
Pontuação de Risco e Certificados Digitais	**APROVADO**		**RESULTADO E OBSERVAÇÃO**
	SIM	**NÃO**	
Demonstrar exibição de condições de risco (Ex. dispositivo com uptime elevado e patch atrasado).			
Escanear certificados digitais instalados e expostos por portas abertas.			
Automação e Playbooks	**APROVADO**		**RESULTADO E OBSERVAÇÃO**
	SIM	**NÃO**	
Criar um playbook com três etapas: verificar espaço em disco → notificar usuário → limpar cache.			
Agendar execução automática com envio de e-mail ao término (não será necessário o envio do e-mail, apenas a comprovação da existência do recurso).			
Experiência do Usuário	**APROVADO**		**RESULTADO E OBSERVAÇÃO**
	SIM	**NÃO**	
Disparar notificação customizada para grupo de dispositivos.			
Aplicar um survey de satisfação via desktop.			

Documento assinado eletronicamente por **Daniel Luzente de Lima**, **Diretor**, em 30/10/2025, às 11:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Elio Thomé de Souza Filho**, **Gerente**, em 30/10/2025, às 11:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 30/10/2025, às 12:01, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 30/10/2025, às 16:35, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **117796170** e o código CRC **E2C270A0**.

Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro, Rio de Janeiro/RJ, CEP 20051-011
Telefone:

Criado por praglb, versão 3 por praglb em 30/10/2025 10:43:39.