Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Vice Presidência de Tecnologia

ESTUDO TÉCNICO PRELIMINAR

PLATAFORMA DE GESTÃO DE IDENTIDADES

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. O PRODERJ, através da Diretoria de Segurança da Informação, na forma do Documento de Oficialização de Demanda instruído no processo, desenvolveu o presente Estudo Técnico de forma a reunir o conjunto de informações indicativas e as condições preliminares exigíveis para a implementação de uma solução de Gestão de Identidades em sua plataforma de segurança e potencial aproveitamento por outros órgãos da Administração Pública, com vistas à mitigação e combate de ameaças de segurança cibernética que afetam a rede governo.

1.2. O ETP ora apresentado constitui etapa do Planejamento da Contratação, regido e tendo por base a Lei Federal 14.133/2021 e demais normativos pertinentes buscando estabelecer as melhores e mais vantajosas condições para o atendimento das demandas necessárias ao adequado funcionamento dos serviços públicos.

1.3. Não obstante o PRODERJ mantenha atualmente em sua infraestrutura de segurança uma solução PAM, que realiza um controle de acessos em nível de administrador, portanto avançado, nas diversas ferramentas presentes na plataforma tecnológica corporativa (firewalls, antivírus, etc), verifica-se a ausência de um instrumento para o controle de acessos de usuários comuns, problema esse que a solução de gerenciamento de identidade e acessos solucionará, permitindo uma visibilidade e um controle de acessos aos usuários do órgão. Utilizando ferramentas como SSO e MFA, essa ferramenta também permitirá a segurança do acesso à sistemas e a rede interna, assim garantindo uma segurança maior para a rede e a identidade dos usuários

1.4. Inserida no campo da Segurança da Informação, a disciplina de Gerenciamento de Identidade e Acessos (IAM) abrange diversas ferramentas que objetivam aumentar os níveis de controle e visibilidade no acesso de usuários. O objeto deste Estudo reúne algumas dessas ferramentas que, se integradas a ferramenta de “Gerenciamento de Acessos Privilegiados (PAM)”, já em uso pelo PRODERJ, proporcionará maior visibilidade e controle, tanto para usuários privilegiados, quanto para os usuários comuns.

1.5. No âmbito público, um dos problemas mais recorrentes são os ataques com foco em roubo de identidade de usuários, realizado através de phishing e outras técnicas. Para combater esse tipo de ataque, ferramentas de gerenciamento de controle de acesso (IAM) se fazem necessárias, de modo a implementar uma camada adicional de segurança, assegurando então a identidade dos usuários e proporcionando visibilidade e controle para a segurança, criando assim um ambiente mais seguro e resiliente a ataques.

1.6. A solução proposta neste Estudo viabilizará o aumento dos níveis de segurança nos acessos de usuários (humanos ou não) no âmbito do PRODERJ, através do controle de elevação de privilégios, MFA, SSO, entre outros, possibilitando então maior visibilidade e controle de acessos aos ativos tecnológicos.

1.7. O PRODERJ, instituição vinculada à Secretaria de Estado de Transformação Digital, atua como Órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro, na forma do art. 3º, do Decreto n° 48.997/2024, que altera a estrutura organizacional do Poder Executivo e reestrutura o Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC. É responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, a segurança da informação, as bases de dados de vários Órgãos estaduais e os diversos equipamentos hospedados no Data Center do Estado. É responsável também por prover serviços de Internet aos Órgãos da administração estadual, tais como correio eletrônico, consultoria, desenvolvimento e hospedagens de páginas, portais, intranets e extranets, bem como conduzir e disponibilizar as atas de registro de preços e contratos corporativos para suprir itens relativos à TIC aos Órgãos e entidades do Estado.

1.8. Diante dessas atribuições e devido ao crescente número de tentativas de invasão e violação de dados que podem levar a perda de informações extremamente importantes, é fundamental que o PRODERJ mantenha os níveis de segurança compatíveis com o papel que desempenha.

1.9. Nos tempos atuais, boa parte dos serviços públicos é ofertada através de sistemas, que permitem acesso rápido à informação, bem como atendimento menos burocrático de seus anseios.

1.10. A evolução dos serviços públicos traz riscos aos prestadores, como o Governo Estadual, que deve se precaver para manutenção do funcionamento ininterrupto de forma segura e sem qualquer tipo de risco.

1.11. A responsabilidade do Estado inclui registro, cadastros, integrações, acessos, inclusões, guardas e tratamentos de informações públicas e privadas dentro do ambiente tecnológico, o que torna o PRODERJ um alvo constante de cyber ataques. A segurança cibernética é fundamental para o perfeito funcionamento do Estado.

1.12. Ademais, essa ferramenta contribuirá para o atendimento da Lei Federal nº 13.709/2018, Lei Geral de Proteção a Dados (LGPD), que intensifica a obrigatoriedade de proteção e privacidade dos dados dos titulares que, no caso da Administração pública, são os cidadãos, o que reforça a necessidade do PRODERJ, Órgão de Tecnologia do Estado, contratar e fornecer aos demais Órgãos da Administração Pública Estadual, uma solução que possa proteger os ativos de TIC contra os diversos tipos de ameaças existentes no mundo cibernético, conforme se observa no seu art. 46:

> 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.

1.13. Por fim, os presentes estudos se embasam nas finalidades institucionais do PRODERJ e sua competência para a promoção de Registro de Preços, em contratações de bens e serviços de TIC, para o atendimento das demandas dos demais órgãos da administração direta e indireta da Administração Pública Estadual, conforme o art. 3º, XIII, do Decreto Estadual nº 48.997/2024.

1.14. O que é o Gerenciamento de Identidade?

1.14.1. As plataformas de gerenciamento de identidade e acesso, também conhecidas como IAM (Identity and Access Management), são um conjunto de processos e tecnologias que permite às organizações controlar e proteger as identidades digitais de seus usuários. Essas identidades podem ser de funcionários, clientes, parceiros ou qualquer outra pessoa que tenha necessidade em acessar sistemas e recursos da empresa. Essa tecnologia ajuda as organizações a reduzir, prevenir, ou, pelo menos, mitigar, os danos decorrentes de ataques externos, bem como de má conduta ou negligência interna.

1.14.2. Embora o gerenciamento de identidade englobe muitas estratégias, um objetivo central é garantir que as pessoas certas tenham acesso aos recursos certos na hora certa, de maneira segura e eficiente, definido como a estrutura de políticas e tecnologias que facilitam a gestão das identidades digitais e os direitos de acesso dos usuários. Isso inclui a autenticação (verificação de identidade), autorização (permissão de acesso) e administração de contas de usuários ao longo de seu ciclo de vida.

1.14.3. O gerenciamento de identidade e acesso é considerado por muitos analistas de tecnologia como um dos processos de segurança mais importantes para reduzir o risco cibernético.

1.14.4. O domínio do gerenciamento de identidade ajuda a fornecer controle, visibilidade, conformidade, auditabilidade refinada sobre todas as identidades.

1.15. O que é identidade?

1.15.1. Identidade, em um contexto de tecnologia da informação, é um conjunto de informações que define e autentica um usuário ou entidade dentro de um sistema. Isso inclui credenciais como nome de usuário, senha, e, em muitos casos, dados biométricos ou tokens de autentificação multifatorial.

1.15.2. A gestão de identidades é crucial para garantir a segurança, integridade e eficiência dos sistemas de TI, prevenindo acessos não autorizados e garantindo que os usuários possam realizar suas tarefas de forma segura e eficiente.

1.16. Contas e senhas compartilhadas

As equipes de TI geralmente compartilham credenciais de root, administrador do Windows e muitas outras credenciais privilegiadas por conveniência, para que as cargas de trabalho e as tarefas possam ser compartilhadas perfeitamente conforme necessário. No entanto, com várias pessoas compartilhando uma senha de conta, pode ser impossível vincular as ações realizadas com uma conta a um único indivíduo. Isso cria problemas de segurança, auditabilidade e conformidade.

1.17. Gerenciamento de identidade manual ou descentralizado

Quando o gerenciamento de identidade é feito manualmente ou de forma descentralizada, há um risco maior de erros humanos, devido à quantidade de usuários e possíveis falhas como senhas fracas ou mal gerenciadas, que podem ser exploradas por atacantes, o que pode comprometer a segurança e conformidade.

1.18. Vetores de Ameaça Privilegiados - Externos e Internos

1.18.1. Ataques de Phishing, Malware, Força Bruta, colaboradores internos desonestos ou descontentes (insiders) e erros de usuários como roubo de credenciais compõem os vetores de ameaças de identidade mais comuns.

1.18.2. Cibercriminosos cobiçam contas de usuários, sabendo que, uma vez obtidas, fornecem um acesso rápido aos sistemas e dados confidenciais de uma organização. Com essas credenciais em mãos, um hacker se torna essencialmente um “colaborador interno” e esse é um cenário perigoso, pois adquirem uma visibilidade dos negócios, sistemas, dentre outros vetores de uma organização. Com essas informações é possível realizar ataques direcionados e ataques de engenharia social para obter mais informações sigilosas.

1.18.3. Ao contrário dos atacantes externos, os colaboradores internos já começam dentro do perímetro, enquanto também se beneficiam do conhecimento de onde estão os ativos e dados confidenciais e como se concentrar neles. As ameaças internas demoram mais para serem descobertas, pois funcionários e outros internos geralmente se beneficiam de algum nível de confiança por padrão, o que pode ajudá-los a evitar a detecção.

1.19. Justificativa

1.19.1. O PRODERJ, instituição vinculada à Secretaria de Estado de Transformação Digital, atua como órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro. É 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. Diante o exposto, se torna essencial a garantia dos três pilares da segurança da informação, preconizada na ISO/IEC 27.000, quais sejam,

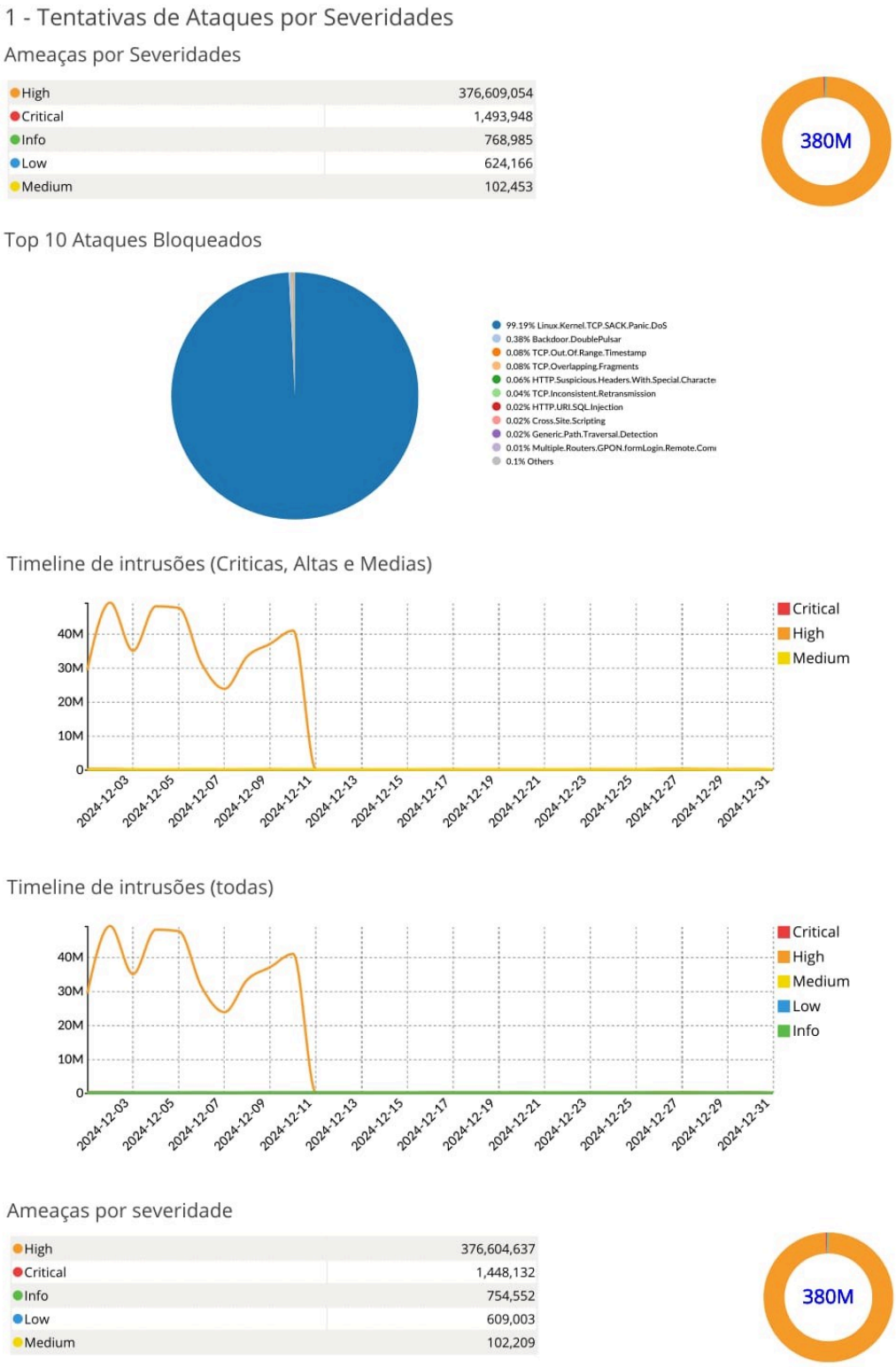
confidencialidade, integridade e disponibilidade das informações. O declínio de apenas um desses pilares, mesmo que momentâneo, em decorrência de tentativas de sequestro de dados ou ataques cibernéticos de qualquer escala, resulta em danos incomensuráveis aos usuários dos serviços prestados através de qualquer sistema. O principal prejudicado é o cidadão, que tem atendidas suas necessidades básicas através de tais serviços.

1.19.2. Cabe também ao PRODERJ a manutenção do Portal Único RJ DIGITAL (Decreto Estadual nº 48.671/2023, art. 7º), com a unificação de informações e serviços prestados pelos órgãos e entidades do Poder Executivo do Estado do Rio de Janeiro.

1.19.3. Diante dessas atribuições é fundamental que o PRODERJ mantenha os níveis de segurança compatíveis com o papel que desempenha.

1.19.4. A tarefa de manter a área de TIC sempre alinhada às estratégias 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 finalísticas da Autarquia. Além desta, existe também a tarefa e obrigação de manter o ambiente tecnológico em alta disponibilidade e de preservar a qualidade dos serviços por ele providos sempre alinhados às estratégias do PRODERJ.

1.19.5. Ante o crescente número de eventos de ataques de agentes malignos vive-se num cenário crítico de segurança cibernética onde os dados institucionais/corporativos estão cada vez mais vulneráveis. Abaixo, relatórios fornecidos pela equipe do SOC da Claro, fornecedora dos links de dados do PRODERJ, referentes ao mês dezembro/2024 com estatísticas de tentativas de ataques ocorridos no período:



2. **RELATO DESCRITIVO DE CONTRATAÇÕES ANTERIORES DE NECESSIDADE IDÊNTICA OU SEMELHANTE, CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES**

2.1. Não existem contratações anteriores de necessidade idêntica observadas no Sistema Integrado de Gestão de Aquisições (SIGA-RJ), realizadas anteriormente pelo PRODERJ.

2.2. O objeto em estudo guarda CORRELAÇÃO com a solução "Senha Segura", objeto correlato sem interdependência, contratado no âmbito do SEI-430002/001692/2024. As duas soluções, se devidamente integradas, tornarão mais segura a relação entre as pessoas e os ativos tecnológicos na infraestrutura do PRODERJ, cada qual em seu foco de atuação: Enquanto a solução de PAM (Senha Segura) atualmente controla os acessos de usuários privilegiados, a solução IAM (deste estudo) controlará os acessos dos demais usuários (não-privilegiados).

2.3. Não obstante, a contratação da solução PAM (Senha Segura) já existente, não sofre INTERDEPENDÊNCIA com a futura e eventual contratação de solução IAM, de forma que uma não depende da outra para ocorrer.

2.5. Saliente-se que a correlação apontada entre os objetos não influencia nas escolhas acerca da solução tecnológica em estudo neste documento (plataforma de gerenciamento de identidades) no que possa tratar de quantitativos pretendidos ou requisitos técnicos necessários.

3. INSTRUMENTOS DE PLANEJAMENTO

3.1. Demonstração da previsão da contratação no Plano de Contratações Anual - PCA do PRODERJ:

a) **ID PCA no PNCP:** 42498600000171-0-000041/2025;

b) **Data de publicação no PNCP:** 01/08/2024;

c) **ID dos itens no PCA do PRODERJ (PNCP):** 24056, 24039, 24046, 24040, 24047, 24041, 24042 e 24043 (itens 1 a 8 respectivamente)

3.2. Previsão no PEDTIC (92294390, p 47 e 48) do PRODERJ:

a) **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);

b) **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);

c) **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);

d) **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. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. Visando manter os níveis desta contratação dentro dos padrões adequados, verifica-se a necessidade de estabelecer, no mínimo, as seguintes exigências:

I - Adicionar uma camada de proteção local e elevação de privilégios, tanto em servidores quanto em estações de trabalho, Autenticação Multifator Adaptativa e Logon Único Adaptativo;

II - Treinamentos operacionais nas soluções contratadas, voltados para os técnicos da Contratante.

III - A solução tecnológica utilizada na prestação dos serviços de subscrição de software (itens 1 a 4 do lote único), deverá estar disponível para acesso do CONTRATANTE por ao menos 99,5% do referido período contratual.

IV - Suporte técnico para todos os componentes da solução, por período igual ao da subscrição, de 12 (doze) meses.

4.2. Requisitos de Capacitação

4.2.1. A capacitação compreende os serviços de treinamentos (itens 5 a 8 do lote único).

4.2.2. O treinamento será direcionado aos técnicos da CONTRATANTE e deverá ser focado na solução adotada e de forma que haja transferência do conhecimento dos recursos em sua totalidade, das configurações existentes e de sua operacionalização.

4.2.3. Na reunião Kick off prevista neste documento, deverá ser entregue para a CONTRATANTE a proposta com o conteúdo do treinamento, para aprovação prévia pela Fiscalização. A referida proposta deverá abordar os pontos constantes deste tópico.

4.2.4. A CONTRATANTE reserva-se o direito de não aceitar o conteúdo do treinamento ou o módulo ministrado, podendo, a seu critério, solicitar a revisão total ou parcial da programação do curso, a troca do de instrutor, caso não sejam satisfatórios. Poderá também ser solicitada a repetição total ou parcial do treinamento, caso não seja satisfatório acerca das exigências aqui contidas.

4.2.5. Deverá ser ministrado por instrutor capacitado na ferramenta, devendo ser comprovado por meio de certificados ou declaração emitida pelo fabricante.

4.2.6. Deverá ser fornecido pela CONTRATADA certificado de capacitação para os participantes do treinamento.

Objetivo

4.2.7. Capacitação do CONTRATANTE para a operacionalização da ferramenta tecnológica.

4.2.8. Formação de facilitadores que possam vir a replicar futuramente o conhecimento no âmbito do CONTRATANTE.

4.2.9. **Métrica**

O treinamento será contratado por turma (2 alunos).

4.2.10. **Carga horária**

4.2.10.1. Deverá ser apresentada pela CONTRATADA, para aprovação da CONTRATANTE, conforme subtópico 4.2.3 acima.

4.2.10.2. Deverá iniciar no prazo máximo de até 20 dias úteis contados da emissão da Ordem de Serviço, quando o CONTRATANTE não especificar prazos no documento.

4.2.10.3. Os treinamentos deverão ser realizados em dias úteis e não poderão exceder o horário comercial.

4.2.10.4. Em casos excepcionais, a critério da Fiscalização, poderão ser solicitados realização dos treinamentos fora do horário comercial, em comum acordo com a CONTRATADA.

4.2.11. **Forma de realização**

O treinamento será em português, ministrado na modalidade remota, em plataforma virtual disponibilizada pela CONTRATADA.

4.2.12. **Materiais didáticos e acessórios**

4.2.12.1. É de responsabilidade da CONTRATADA arcar com todo material audiovisual, didático e eletrônico para a realização dos treinamentos, e quaisquer outras despesas diretas ou indiretas relacionadas ao tema.

4.2.12.2. O material didático será fornecido em português, pela CONTRATADA, abordando todos os tópicos do curso.

4.2.13. **Conteúdo programático**

4.2.13.1. O treinamento deverá englobar a realização de laboratórios práticos, fornecidos pela CONTRATADA, para configuração e execução de exercícios práticos na mesma versão dos produtos ofertados.

4.2.13.2. Deverá abordar, no mínimo: o uso da ferramenta, instalação, configuração, operação da ferramenta, gerenciamento, resolução de problemas, e deverá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE.

4.2.13.3. Deverá contemplar todos os recursos e configurações existentes na solução ofertada.

4.3. Requisitos Legais

Sem previsão de normatização específica pertinente ao objeto em estudo.

4.4. Requisitos de Manutenção

4.4.1. Todas as rotinas para fins de manutenção com vistas ao pleno e adequado funcionamento das soluções ao longo da vigência contratual estará a cargo da CONTRATADA na forma do Suporte Técnico previsto no subtópico 4.9.4 deste documento. O referido Suporte Técnico contempla a manutenção corretiva com o objetivo solucionar defeitos encontrados no software, e também a manutenção evolutiva na forma da atualização oportuna das soluções contratadas.

4.4.2. A CONTRATADA deve disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.

4.4.3. Os chamados abertos deverão obedecer aos níveis de serviço estabelecidos na tabela do subtópico 4.9.4.6 deste documento.

4.5. Requisitos Temporais

Resguardado o cronograma previsto no subtópico 25.2 deste documento, não havendo outros requisitos temporais a serem considerados.

4.6. Requisitos de metodologia de trabalho

4.6.1. Serão instrumentos formais de comunicação entre a CONTRATANTE e a CONTRATADA:

a) Ordens de Serviço;

b) Plano de Inserção;

c) Termos de Recebimento;

d) Chamado registrado na Central de Atendimento;

e) Ofícios;

f) Relatórios e Atas de Reunião;

g) E-mail;

h) Demais Termos que venham a ser previstos no instrumento convocatório.

4.6.2. A execução de quaisquer dos itens previstos no lote único será sempre precedida da emissão de Ordem de Serviço – O.S., contendo no mínimo: descrição do serviço, quantitativo, prazo para a execução do serviço, período para a execução do serviço, local da execução do serviço e especificações técnicas do serviço esperados.

4.6.3. A comunicação entre a CONTRATANTE e a CONTRATADA, para fins de encaminhamento de Ordens de Serviço ou outro documento, ocorrerá sempre por intermédio do preposto, ou seu substituto, designado pela CONTRATADA;

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

4.6.5. O horário de funcionamento do órgão é entre 08hs e 18hs, de segunda a sexta-feira, resguardadas eventuais emergências cuja ocorrência se dê em qualquer horário e dia.

4.6.6. O acesso de representante da contratada nas dependências da contratante, deverá ocorrer mediante prévia comunicação entre as partes, por meio dos mecanismos de comunicação definidos neste instrumento.

4.7. **Requisitos de Segurança da Informação e Privacidade**

4.7.1. Caso se faça necessário, para um eventual suporte nas dependências da CONTRATANTE, a CONTRATADA deverá exigir dos seus empregados, o uso obrigatório de uniformes e crachás de identificação.

4.7.2. Caso se faça necessário, para um eventual suporte nas dependências da CONTRATANTE, a CONTRATADA não poderá se utilizar da presente situação para obter qualquer acesso não autorizado às informações de propriedade da CONTRATANTE.

4.7.3. A CONTRATADA não pode obter, capturar, copiar ou transferir qualquer tipo informação de propriedade do CONTRATANTE, sem autorização.

4.7.4. A CONTRATADA deve atender à Política de Segurança da Informação instituída pela Instrução Normativa PRODERJ PRE nº 02, de 28 de abril de 2022, e demais normativos correlatos publicados pelo CONTRATANTE.

4.7.5. **Proteção de Dados Pessoais**

4.7.5.1. No cumprimento dos serviços de subscrição de software (itens 1 a 4 do lote único) haverá entre CONTRATANTE e CONTRATADO o compartilhamento das seguintes informações de funcionários da CONTRATADA a atuarem nas etapas de implementação:

a) nome completo;

b) número de ID ou matrícula funcional;

c) endereço de e-mail.

4.7.5.2. No cumprimento dos serviços de treinamento (itens 5 a 8 do lote único) haverá entre CONTRATANTE e CONTRATADO o compartilhamento das seguintes informações dos funcionários a serem treinados:

a) nome completo;

b) número de ID ou matrícula funcional;

c) endereço de e-mail funcional;

d) CPF (em razão da emissão de certificados de conclução/aprovação).

4.7.5.3. É vedado ao CONTRATADO o compartilhamento com terceiros das informações de funcionários da CONTRATANTE, excetuado o respectivo fabricante da solução a ser treinada no caso de uso de plataforma de aulas por ela mantida.

4.7.5.4. Ao final do vínculo contratual, resguardadas quaisquer disposições na Lei Geral de Proteção de Dados e eventuais entendimentos consolidados pela Autoridade Nacional de Proteção de Dados, o CONTRATADO deverá providenciar o descarte definitivo dos dados pessoais aqui referidos.

4.8. **Requisitos Sociais, de Sustentabilidade Ambiental e Culturais**

4.8.6. Não se observa a existência de critérios de sustentabilidade ambiental ou requisitos sociais e culturais previamente definidos ou relativos ao objeto proposto neste documento.

4.8.7. Não obstante, a CONTRATADA deverá, no que for aplicável, obedecer aos critérios estabelecidos no Decreto Estadual nº 43.629/2012.

4.9. **Requisitos Tecnológicos**

4.9.1. **De arquitetura tecnológica**

4.9.1.1. Os requisitos tecnológicos de arquitetura da solução, relacionados aos itens 1 a 4 do lote único, encontram-se no Anexo I Especificações Técnicas do Objeto, bem como nas disposições acerca da Reunião Kick Off no subtópico 4.9.3.1 deste documento.

4.9.1.2. Os requisitos relacionados ao serviço de treinamento (itens 5 a 8 do lote único), encontram-se no subtópico 4.2. (Requisitos de Capacitação) deste documento.

4.9.1.3. O ciclo de vida das soluções tratadas neste documento refere-se ao período entre o início de operação, na infraestrutura do CONTRATANTE, das soluções de software previstas, durante o qual o fabricante fornece suporte e atualizações para o produto, até a expiração das licenças de uso das referidas soluções.

4.9.2. **Do projeto**

4.9.2.1. Compreende-se nesta etapa a instalação e configuração das soluções contratadas, fornecidos nos itens 1, 2, 3 e 4 do Lote Único, bem como a migração das configurações existentes na CONTRATANTE para os produtos fornecidos pela CONTRATADA;

4.9.2.2. A etapa de instalação e configuração deve acontecer de forma gradual e transparente, de acordo com a conveniência da CONTRATANTE.

4.9.2.3. Durante esta etapa, a equipe da CONTRATADA deverá estar presente nos horários de testes, implantação e migração, definidos pela CONTRATANTE.

4.9.2.4. As atividades de instalação e configuração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana.

4.9.2.5. Durante a etapa de instalação e configuração, os produtos fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção.

4.9.2.6. A CONTRATADA deverá, com a supervisão e aprovação da CONTRATANTE, planejar e realizar a instalação e configuração dos softwares com total interoperabilidade no ambiente atual da CONTRATANTE, sem impacto no ambiente de produção.

4.9.2.7. Durante a implantação e integração, caso seja aplicável/necessário, a CONTRATADA deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas e implementação de segurança.

4.9.2.8. Para instalação e configuração devem ser consideradas as seguintes premissas:

I - Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares e recursos humanos necessários à instalação das soluções;

II - Caberá à CONTRATADA disponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da CONTRATANTE caso a instalação dos produtos / softwares da CONTRATADA apresente falha.

III - A CONTRATADA deverá fornecer todas as licenças necessárias dos PRODUTOS ofertados e dos elementos adicionais que se fizerem necessários à instalação e ao pleno funcionamento do ambiente de produção.

4.9.2.9. A CONTRATADA deverá submeter previamente, por escrito, à CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações acordadas.

4.9.2.10. O encaminhamento formal das demandas, considerados cada um dos itens do objeto ocorrerá sempre por meio de emissão da Ordem de Serviço.

4.9.3. **Da implantação**

4.9.3.1. A CONTRATADA deve realizar, nas dependências da CONTRATANTE, antes do início da implantação da solução, uma reunião inicial de projeto (kick-off) em conjunto com as áreas de Segurança da Informação e infraestrutura da Contratante para definir o Plano de Trabalho de instalação e configuração da solução.

4.9.3.2. Durante a reunião de kick-off a CONTRATADA deverá especificar a arquitetura do software para a CONTRATANTE a fim de que sejam realizadas as providências necessárias para a adequação do ambiente e consequente funcionamento da solução. Tais procedimentos devem estar alinhados às especificações técnicas descritas no Anexo I - Especificações Técnicas do Objeto, deste documento.

4.9.3.3. Após a reunião de kick-off a CONTRATADA deverá produzir e entregar ao CONTRATANTE o Projeto Executivo elaborado com base no quanto acertado ao longo da reunião, 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 Contratante.

4.9.4. **Do suporte técnico / Garantia dos serviços**

4.9.4.1. Durante todo o período da subscrição, a CONTRATADA será responsável pelo suporte técnico da solução tecnológica composta pelos itens 1 a 4 do Lote Único a título de garantia dos serviços prestados.

4.9.4.2. Em caso de interrupção ou indisponibilidade das soluções, a CONTRATADA se compromete a realizar as correções necessárias à reativação da mesma, e a prevenção de novas interrupções, respeitando os prazos de atendimento.

4.9.4.3. Entende-se por “indisponibilidade total” quando a solução não está acessível, e “indisponibilidade parcial” quando há degradação dos serviços.

4.9.4.4. A CONTRATADA deverá disponibilizar por meio da Internet uma aplicação WEB para registro dos chamados de suporte técnico através de login e senha fornecida para os usuários autorizados da contratante, em regime de 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados).

4.9.4.5. Os chamados abertos por órgão CONTRATANTE no sistema de chamados da CONTRATADA não poderão ser visualizados por outros órgãos contratantes.

4.9.4.6. Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado no sistema, observados os níveis de severidade, na forma da tabela abaixo:

TABELA 3

Severidade	Descrição	Tempo do 1º contato após abertura do chamado	Tempo de solução
alta	Objeto totalmente inoperante	até 30 minutos	até 4 horas
média alta	Solução parcialmente inoperante: necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 2 horas	até 10 horas
média	Solução não inoperante, mas com problema de funcionamento: necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução	até 6 horas	até 72 horas
baixa	Solicitações de informações diversas ou dúvidas sobre a solução	até 8 horas	até 120 horas

4.9.4.7. O suporte técnico deverá contemplar manutenção corretiva e evolutiva e não poderá acarretar custos adicionais ao CONTRATANTE.

- Entende-se por manutenção corretiva uma série de procedimentos destinados a recolocar a solução em pleno estado de funcionamento, removendo definitivamente os defeitos apresentados.
- Entende-se por manutenção evolutiva a atualização do sistema por meio do fornecimento de novas versões e/ ou releases corretivas e/ou evolutivas de softwares que compõem a solução, que venham a ser lançadas durante a vigência do contrato.

4.9.4.8. Considera-se plenamente solucionado o problema quando restabelecidos os sistemas/serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa.

4.9.4.9. A contratante poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência do contrato. A contratada deverá inclusive, ter acesso ao suporte técnico do fabricante da solução, caso haja a necessidade de escalar algum problema, tendo em vista garantir o serviço prestado.

4.9.4.10. Ao final de cada mês será emitido um relatório gerencial e técnico com todas as informações sobre os atendimentos realizados, contendo a identificação do problema, providências adotadas e demais informações pertinentes.

4.9.4.11. A contratada será responsável por possíveis migrações para novas versões da solução oferecida, sempre que demandadas pelo contratante.

4.9.4.12. A CONTRATANTE poderá, a qualquer momento, solicitar a substituição imediata dos técnicos envolvidos no atendimento caso julgue ineficiente os resultados inerentes à prestação de serviço e resolução dos problemas. Nestes casos, a CONTRATADA terá um prazo de até 48 (quarenta e oito) horas úteis para a substituição da equipe de atuação.

4.9.4.13. A CONTRATADA poderá solicitar a prorrogação de quaisquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado. Caberá a CONTRATANTE aceitar ou não o pedido de prorrogação do prazo.

4.9.4.14. O horário de funcionamento do órgão é entre 08hs e 18hs, de segunda a sexta-feira, resguardadas eventuais emergências cuja ocorrência se dê em qualquer horário e dia.

4.9.4.15. O acesso de representante da contratada nas dependências da contratante, deverá ocorrer mediante prévia comunicação entre as partes, por meio dos mecanismos de comunicação definidos neste instrumento.

4.9.5. **De experiência da equipe que executará os serviços relacionados à solução de TIC e formação da equipe que projetará, implementará e implantará a solução de TIC**

4.9.5.1. As necessidades de mão de obra especializada estão diretamente relacionadas com a instalação/configurações, o suporte técnico da solução e o treinamento.

4.9.5.2. A equipe a ser utilizada pela CONTRATADA no cumprimento do objeto, deverá comprovadamente, para fins de contratação, ser qualificada e com experiência nas atividades previstas no objeto.

4.9.5.3. Serão aceitas cópias dos certificados ou diplomas que comprovem as formações e /ou experiências exigidas.

4.10. **Requisitos Materiais e Humanos**

4.10.1. Materiais, insumos e acessórios necessários ao perfeito funcionamento das soluções previstas no lote único deverão ser arcados pela CONTRATADA, sem custos adicionais para o CONTRATANTE.

4.10.2. 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, que contempla serviços de treinamento e subscrição de solução tecnológica, não prevê o uso de mão de obra residente/dedicada nas dependências do órgão contratante. Adicionalmente registre-se que o objeto também não caracteriza, forma alguma, terceirização de atividade-fim, tendo em vista que se trata de contratação, em regime de locação/subscrição de software e respectivos cursos de treinamento, bem como suporte técnico específico do fabricante/fornecedor representante, que estão diretamente relacionados à atuação de profissionais e especialistas nas soluções contratadas.

4.10.3. **Restrições de área, identificando questões de segurança institucional, privacidade, segurança, medicina do trabalho, dentre outras:**

Na forma do subtópico 4.7.4 deste documento.

4.10.4. **Disposições normativas internas:**

Na forma do subtópico 4.7.4 deste documento.

4.10.5. **Instalações, especificando-se a disposição de mobiliário e equipamentos, arquitetura, decoração, dentre outras:**

Na forma do subtópico 4.9.3 deste documento.

5. **LEVANTAMENTO DE MERCADO**

5.1. **Levantamento das Soluções**

5.1.1. **Soluções para Gestão de Identidades**

5.1.1.1. Em observação de contratações similares, demonstradas na tabela do tópico 6 deste documento, verifica-se que todos os processos tratam de subscrição de software (variando apenas o período), ou seja, não observa nenhuma referência de contratações públicas em modalidade “aquisição perpétua”. Na análise de documentos técnicos dos principais fabricantes atuantes no mercado, se confirma a evidência de que a prática usual de mercado vem sendo a subscrição de software.

5.1.1.1. Verifica-se os cenários possíveis para o atendimento da demanda, conforme segue:

I - **Solução 1 - Solução Open Source:** Existem no mercado soluções gratuitas e/ou open source que possuem as características técnicas que possibilitariam o atendimento da presente demanda, como por exemplo o “OpenIAM”, “MidPoint”, “FusionAuth”, dentre outros.

- Vantagem: Ferramentas gratuitas e disponíveis na internet não envolvem custos diretos com a contratação de serviço ou solução tecnológica, inclusive quanto à instalação e suporte da ferramenta.
- Desvantagem: As soluções gratuitas e/ou open source carecem de suporte técnico adequado ao ambiente corporativo, e trazem ainda a desvantagem da necessidade em se operar mais de uma solução tecnológica para a obtenção de todas características técnicas desejadas no objeto. Há de se destacar ainda o risco de descontinuidade da solução, pois dado o caráter gratuito do software, o fabricante não estaria obrigado a dar suporte e atualizações para uma solução descomissionada.

II - **Solução 2 - Contratação da solução de Gerenciamento de Identidades no modelo Pay-as-you-go (Pague pelo uso):** Neste cenário, o PRODERJ contrata a solução pelo método pay-as-you-go, ou seja, o Contratante paga apenas o que consumir. Este tipo de contratação é flexível pelo fato do valor a ser pago ser definido conforme a sua utilização, sendo comum em ambientes e soluções baseadas em nuvem. No caso da solução de IAM, a cobrança pode ser abordada no modelo de usuários ativos, com base na quantidade de usuários que acessaram o ambiente, ou ainda por meio de transação ou evento, onde a cobrança é feita através da quantificação das autenticações realizadas (por MFA, SSO, entre outros). Este modelo

de contratação é comum no setor privado, onde os serviços de IaaS são mais utilizados. Este modelo de negócio é adotado por provedores de nuvem como Amazon AWS, Microsoft Azure e Google Cloud.

- Vantagem: Este modelo de contratação permite que o Contratante possa reduzir o valor de sua fatura mensal com o as licenças utilizadas, pois a escalabilidade dinâmica proporcionada pelo modelo permite a redução ou acréscimo de licenças utilizadas de maneira imediata, o que pode gerar economia com licenças ociosas.

- Desvantagem: Este modelo é aplicado apenas a ambientes de nuvem (IaaS), sendo restrito a nuvem daquele mesmo provedor de IaaS, o que é um fator limitante, especialmente em ambientes multi-cloud. Para além das questões técnicas, este modelo de contratação não é comum no setor público, pois as flutuações nas faturas mensais prejudicam o planejamento orçamentário do Contratante.

III - **Solução 3 - Contratação de solução de Gerenciamento de Identidade através de Serviço Gerenciado:** Nesse cenário, a Contratada é responsável pela gestão, configuração e operação da solução de IAM, inclusive a implementação no ambiente da Contratante. A Contratada seria responsável ainda pela resolução de outras questões relacionadas à ferramenta, como integração com outros sistemas e adequação da ferramenta com as conformidades regulatórias pertinentes. Neste modelo de contratação, é comum também o monitoramento e suporte 24/7, com o intuito de aumentar a segurança fornecida sem que haja atrasos nas respostas.

- Vantagem: Toda a operação, implementação, suporte e monitoramento da ferramenta ficaria a cargo da CONTRATADA, e o papel do Contratante seria fornecer as orientações para a operação da solução, o que poderia acontecer a qualquer tempo durante o período contratual. Este modelo também possui a vantagem de aliviar a equipe técnica do Contratante, uma vez que a operação cotidiana da solução demandará ajustes constantes na configuração, que serão realizados pela Contratada.

- Desvantagem: Neste cenário, uma vez que a empresa Contratada é a responsável pelo gerenciamento da ferramenta, o Contratante estaria em situação de total dependência em relação à Contratada, pois no modelo de Serviço Gerenciado, é comum a ausência de treinamento na solução, que perde o sentido se a ferramenta é operada por terceiros. Outra desvantagem relevante é a diferença de preços entre o serviço gerenciado e a mera subscrição do software, onde o primeiro pode ser consideravelmente mais caro que o segundo (vide tabela do tópico 10.5 deste documento).

IV - **Solução 4 - Contratação de subscrição de Plataforma de Gerenciamento de Identidades**

Neste cenário, ocorre a contratação da referida Plataforma na modalidade subscrição de software, com a instalação da solução inclusa, se configurando em prestação de serviço de natureza contínua. O modelo viabiliza agregar à solução o respectivo serviço de treinamento operacional, destinados aos técnicos da contratante.

- Vantagem: A implementação da ferramenta ficaria a cargo da Contratada, que terá condições, graças a sua expertise com a Solução, de realizar o procedimento de maneira mais assertiva. Neste cenário, a Contratada estaria também obrigada a prestar suporte técnico para a solução contratada, garantindo a plena operação da solução durante o período da subscrição. E por fim, as soluções enterprise, via de regra, possuem todas as principais características técnicas necessárias ao ambiente corporativo, evitando assim o uso de múltiplas soluções que poderiam estar centralizadas em apenas uma.

- Desvantagem: A Contratante deverá se antecipar ao vencimento do contrato de subscrição, sob pena de perder o direito de uso da solução, caso não providencie novo contrato a tempo.

5.1.2. **Soluções de Treinamento**

5.1.2.1. É comum se observar em contratações de soluções tecnológicas a demanda pelo respectivo treinamento, uma vez que se faz necessária a capacitação dos quadros técnicos do CONTRATANTE para a correta opercionalização da nova ferramenta. Essa capacitação pode vir como aspecto intrínseco da solução ou como item destacado e neste último caso, pode vir em modelo individual (por aluno) ou por turma para um determinado número de alunos. Os estudos técnicos conduzidos pelo PRODERJ com vistas a obtenção de soluções tecnológicas diversas costumam considerar está mesma lógica.

5.1.2.2. Todavia, nos projetos similares observados (vide tópico 6 deste documento) se verifica em alguns casos a previsão de treinamento como elementos intrínseco da solução (83754136 e 83752730) ou como item destacado medido por turma de 2 alunos (83752096). Não se verifica em nenhum a ocorrência de treinamento por aluno e em alguns sequer há a previsão de treinamento (83753910, 83754130 e 83752105).

5.1.2.3. Com efeito, não se vislumbra desconsiderar a previsião de treinamento para a solução em estudo, uma vez que representa solução não conhecida pelos quadros técnicos desta autarquia, bem como a possibilidade de licitação em Sistem de Registro de Preços para a participação de outros órgãos da Administração, os quais poderão ou não apresentar quadros técnicos já treinados para a solução em tela.

5.1.2.4. Também foi descartado como opção o treinamento como parte intrínseca da solução tendo em vista que, enquanto objeto em modalidade serviço com possibilidade de renovação após 12 (doze) meses, a cada renovação do objeto como um todo, o CONTRATANTE estaria pagando também pelo treinamento, ainda que dele não mais venha a precisar. Ademais, considerada a hipótese de licitação em SRP, cada participante/aderente, ainda que sem necessitar do treinamento, teria que absorvê-lo junto com a solução.

I - **Treinamento como item destacado com unidade de medida por aluno**

- Vantagem:
  - Personalização: Permite que os alunos escolham horários ou turmas que melhor se adequem às suas agendas;
  - Custo escalável: Se apenas alguns funcionários precisam do treinamento, o investimento é menor;
  - Diversidade de turmas: Os alunos podem ser alocados em turmas com participantes de outras empresas, o que pode enriquecer a troca de experiências.
- Desvantagem:
  - Custo elevado para grandes equipes: Se muitos colaboradores precisam ser treinados, o valor total pode ser alto;
  - Falta de alinhamento interno: Como os alunos podem estar em turmas diferentes, o aprendizado pode não ser uniforme;
  - Logística complexa: Gerenciar várias inscrições individuais pode ser trabalhoso;
  - Menos foco nas necessidades da empresa: O conteúdo pode ser mais genérico, já que o treinamento não é exclusivo para sua equipe.

II - **Treinamento como item destacado com unidade de medida por turma**

- Vantagem:
  - Custo-benefício: Ideal para treinar muitos colaboradores de uma só vez, reduzindo o custo por aluno;
  - Conteúdo personalizado: O treinamento pode ser adaptado às necessidades específicas da empresa e do projeto;
  - Alinhamento da equipe: Todos os participantes recebem o mesmo conteúdo, o que facilita a implementação da solução tecnológica;
  - Maior engajamento: A dinâmica de grupo pode aumentar a motivação e a interação entre os colaboradores;
  - Facilidade logística: A empresa só precisa organizar um único treinamento.
- Desvantagem:
  - Dificuldade de agendamento: Encontrar um horário que funcione para todos os participantes pode ser desafiador;
  - Menor flexibilidade: Se novos colaboradores precisarem ser treinados posteriormente, será necessário contratar outro treinamento;
  - Risco de desuniformidade: Se a turma for muito grande, alguns alunos podem não receber a atenção necessária.

5.2. **Avaliação Comparativa (Benchmarking)**

A seguir, tabela comparativa com alguns fabricantes líderes de mercado. Nas tabelas, são elencadas algumas características técnicas relevantes para a referida tecnologia.

Benchmark - Identity and Access Management - IAM (agosto de 2024)					
Feature	**FABRICANTES**				
	IBM	**MICROSOFT**	**CYBERARK**	**ORACLE**	**ENTRUST**
SSO	SIM	SIM	SIM	SIM	SIM
MFA	SIM	SIM	SIM	SIM	SIM
App Gateway	NÃO*	SIM	SIM	NÃO*	NÃO*
Controle de Identidade e Acessos via um autenticador da ferramenta	NÃO*	SIM	SIM	NÃO*	NÃO*
Acesso Adaptativo**	SIM	SIM	SIM	NÃO*	SIM
Proteção para recursos On-Premisse	SIM	SIM	SIM	SIM	SIM
Proteção para recursos baseados em nuvem	SIM	SIM	SIM	SIM	SIM
Integração com outras ferramentas PAM	NÃO*	SIM	SIM	SIM	NÃO*
Todas as features na mesma ferramenta	SIM	SIM	SIM	SIM	SIM
* feature não localizada nos detasheets das soluções					
** Compatibilidade com ambiente Zero Trust relacionado à identidade do usuário					

5.2.1. **Disponibilização de IRP para a solução pretendida**

Não se verifica IRP - Intenção de Registro de Preços em condução no SIGA-RJ para fins de contratação da solução proposta neste documento. Não obstante, convém salientar que as demandas do PRODERJ, em aquisição de soluções de Tecnologia da Informação e Comunicação, contemplam também as demandas dos demais órgãos da Administração Estadual, uma vez que, por força do Decreto nº 48.997/2024, art. 3º, o PRODERJ é o diretor-geral do Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC, no âmbito do Governo do Estado do Rio de Janeiro, com a competência para conduzir a governança, a gestão, o planejamento, a definição de estratégias, a normatização e a supervisão do sistema, inclusive para a adoção de padrões concernentes a equipamentos de informática e de comunicação de dados, de rede, de segurança e de aplicativos de automação de escritórios, podendo, para tanto, realizar os procedimentos para contratação das soluções, bem como outros serviços e bens de natureza de tecnologia da informação e comunicação para atendimento das necessidades dos órgãos estaduais e suas vinculadas, preferencialmente por ata de registro de preço. Por fim, saliente-se que conforme previsto no citado Decreto, é do PRODERJ a competência para oferta de IRP para fins de licitação de soluções tecnológicas com a tratada neste estudo técnico.

6. **ANÁLISE DE PROJETOS SIMILARES**

Na tabela a seguir, a análise qualitativa de contratações similares encontradas no Portal da Transparência, mantido pela Controladoria Geral da União, bem como nos sítios virtuais dos respectivos órgãos.

	órgão / entidade	nº contrato / edital	valor da proposta / contrato (R$)	fornecedor	natureza do objeto	duração do contrato	análise da contratação	vantagens	desvantagens
01	Assembleia Legislativa do Estado do Rio Grande do Norte	P.E. nº 49/2023 (83753910)	R$ 4.962.306,10	F9C Security LTDA	serviço (subscrição)	12 meses	O objeto do lote único é composto pela subscrição de diversas soluções de segurança: IAM, PAM, proteção de e-mail e teste de intrusão, mais os serviços de suporte associados a cada licença. Apenas o item 3.1 do objeto trata sobre a mesma tecnologia abordada neste estudo. A solução não apresenta item referente a Treinamento.	O órgão contratante em apenas um processo de contratação pôde resolver o fornecimento de diversas soluções de segurança.	O objeto apresenta alguns itens poderiam estar em lotes separad como a solução para proteção de mail e os testes de intrus Adicionalmente, entende-se que item de suporte técnico (3.2.) pod estar agregado ao item da subscriç a exemplo de diversas contrataç do PRODERJ.
02	Prefeitura Municipal de Anápolis - GO	P.E. nº 10/2023 (83754130)	R$ 2.586.620,96 (valor estimado no edital)	---------	serviço (subscrição)	12 meses	O objeto apresenta equivalência a todos os componentes tecnológicos do presente objeto, além da mesma modalidade de contratação, por subscrição de software. A solução não apresenta item referente a Treinamento.	Os itens 1, 2, 4, 5 e 6 do processo analisado possuem especificações técnicas semelhantes às das tecnologias abordadas neste estudo.	Os itens 4 e 5, que tratam essencialmente do mesmo tipo ativo (servidores), estão separad sendo um item para servid Windows e outro para servid Linux. Observa-se no mercado existem soluções que abrangem dois tipo de sistema operacional.
03	Tribunal de Contas do Estado do Maranhão	P.E. nº 23/2023 (83754136)	R$ 2.974.800,00	GLOBAL Sec. Tecnologia & Informação LTDA	serviço (gerenciado pela contratada)	12 meses	O objeto do lote único é composto por 6 itens de serviço gerenciado, mais 6 itens correspondentes a instalação da solução, mais 1 item de serviço especializado, totalizando 13 itens reunidos em lote único. O treinamento se apresentada como aspecto intrínseco da solução como um todo.	O órgão contratante, em apenas um processo de contratação, pôde resolver o fornecimento de diversas soluções de segurança, embora tal escolha na composição do objeto não seja compatível com uma ARP.	O objeto apresenta, no mesmo l itens que envolvem diver tecnologias e soluções distintas, e poderiam então constar em l distintos. No caso do item 6, apresenta semelhança com um nossos itens, a instalação consta item separado, o que entende-se co desnecessário.
04	Serviço Nacional de Aprendizagem do Cooperativismo - SESCOOP	P.E. nº 06/2022 (83752096)	R$ 2.751.402,48	NTSEC Soluções em Teleinformática LTDA	serviço (subscrição)	36 meses	O objeto é composto por 7 lotes, mas apenas os itens do lote 1 correspondem a mesma tecnologia abordada neste estudo. No lote em questão, a contratação é via subscrição de ferramenta SaaS. O serviço de treinamento está previsto em modalidade turma para 2 pessoas.	A opção pela renovação das licenças de uma solução já em uso evitará muitos problemas operacionais oriundos de possíveis trocas de solução.	Talvez por se tratar da renovação um serviço já implementado, especificações técnicas do objeto Termo de Referência for suprimidas, o que impossibi qualquer análise técnica n aprofundada sobre o processo.
05	Tribunal Regional Eleitoral do Paraná - TRE/PR	P.E. nº 63/2022 (83752105)	R$ 3.350.961,36	APPROACH Tecnologia LTDA	serviço (subscrição)	36 meses	O objeto do lote único é composto por itens de subscrição de tecnologias IAM e PAM. Os itens 1 e 4 do objeto do lote único, aparentam semelhança com a tecnologia abordada neste estudo. A solução não apresenta item referente a Treinamento.	A opção pela renovação das licenças de uma solução já em uso evitará muitos problemas operacionais oriundos de possíveis trocas de solução.	Talvez por se tratar da renovação um serviço já implementado, especificações técnicas do Termo Referência foram reduzidas a me de uma página.
06	Banco do Estado do Pará - BANPARÁ	P.E. nº 28/2023 (83752730)	R$ 36.101.641,00	3STRUCTURE IT LTDA	serviço (subscrição)	48 meses	O objeto do lote único trata da subscrição de licenças de software, tendo em vista a renovação das licenças atualmente em uso na Instituição. O treinamento se apresentada como aspecto intrínseco da solução como um todo.	A opção pela renovação das licenças de uma solução já em uso evitará muitos problemas operacionais oriundos de possíveis trocas de solução.	Talvez por se tratar da renovação um serviço já implementado, especificações técnicas do Termo Referência foram reduzidas a u página.

7. **ESPECIFICAÇÃO DE MARCA/FABRICANTE**

7.1. Não se aplica a especificação de marcas ou modelo, nem vedação de utilização de marca ao presente estudo.

7.2. Saliente-se a ausência de previsão legal para a indicação de marca em objetos que não envolvam o fornecimento de bens (art. 41, caput, da Lei Federal nº 14.133/2021).

8. **MÉTRICA PARA MENSURAÇÃO DOS SERVIÇOS**

Na forma do Acordo de Nível de Serviço previsto no subtópico 26.1 deste documento.

9. **ESTIMATIVAS DAS QUANTIDADES A SEREM CONTRATADAS**

9.1. A tabela abaixo apresenta as quantidades estimadas da solução conforme as demandas do PRODERJ.

Lote único					
Nº do Item	**ID SIGA**	**ID PCA**	**Descrição do Bem ou Serviço**	**Métrica**	**Quantidade estimada**
1	189256	24056	Subscrição de Licença para Proteção Local e Elevação de Privilégio em servidores, com suporte técnico, por de 12 (doze) meses	Unidade	2.116
2	189257	24039	Subscrição de Licença para Proteção Local e Elevação de Privilégio em desktops, com suporte técnico, por 12 (doze) meses	Unidade	540
3	189258	24046	Subscrição de Solução de Autenticação Multifator Adaptativa, com suporte técnico, por 12 (doze) meses	Unidade	758
4	189259	24040	Subscrição de Solução de Logon Único Adaptativo para Identidades dos Colaboradores, com suporte técnico, por 12 (doze) meses	Unidade	758
5	189263	24047	Treinamento operacional para solução de Proteção Local e Elevação de Privilégio em servidores	Turma	6
6	189264	24041	Treinamento operacional para solução de Proteção Local e Elevação de Privilégio em desktops	Turma	6
7	189265	24042	Treinamento operacional para solução de Autenticação Multifator Adaptativa	Turma	6
8	189266	24043	Treinamento operacional para solução de Logon Único Adaptativo para Identidades dos Colaboradores	Turma	6

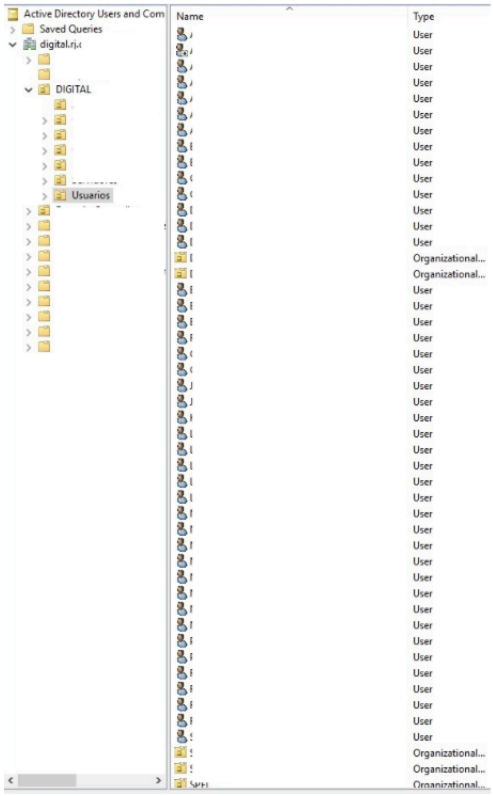
9.2. **Forma de quantificação das demandas do PRODERJ:**

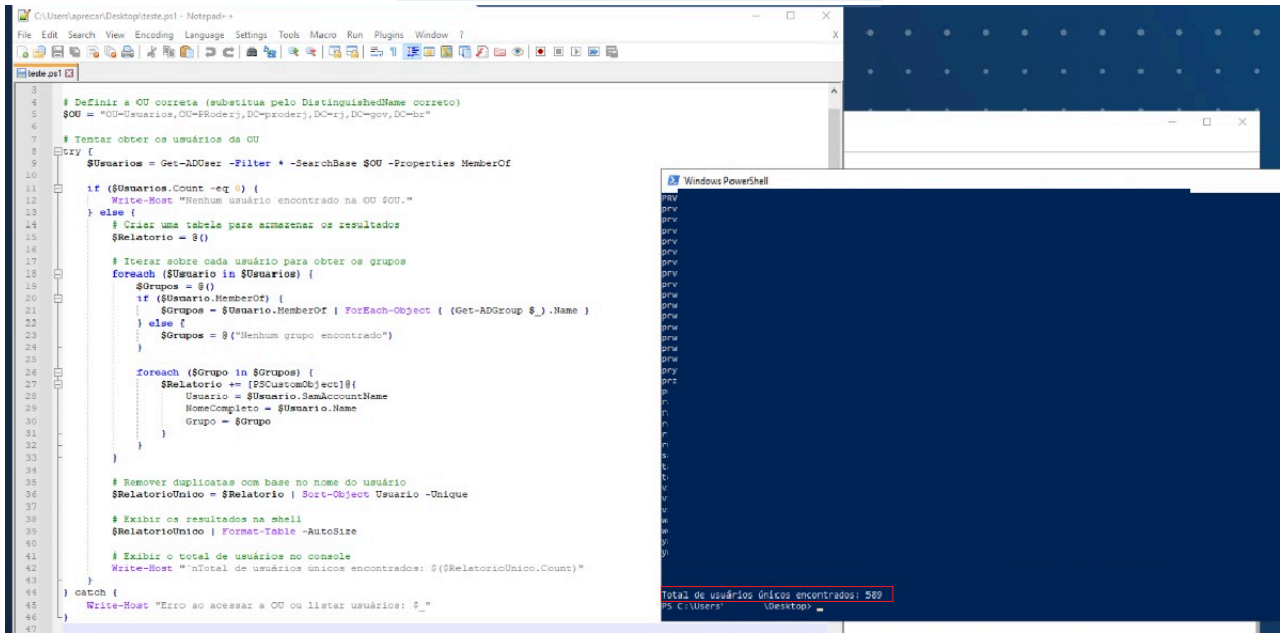
9.2.1. O quantitativo informado na tabela acima foi elaborado levando em conta a infraestrutura atual do PRODERJ, e os dados que embasam a tabela foram extraídos da base de usuários do Active Directory e da ferramenta XDR. Assim, a referida quantificação considera a atual infraestrutura da Autarquia, conforme abaixo:

I - **Item 1**: se faz necessário 1 (uma) unidade por servidor Windows e Linux, físicos ou virtuais sob responsabilidade do PRODERJ, conforme apontado pela Gerência de Infraestrutura e Serviços (DIT/GIS) no somatório de clusters informados no item 1 do seu despacho (93684629).

II - **Item 2**: se faz necessário 1 (uma) unidade por estação de trabalho existente na infraestrutura PRODERJ, conforme apontado pela Gerência de Suporte Técnico (DIT/GST) no seu despacho (93685530).

III - **Item 3:** se faz necessário 1 (uma) unidade para cada usuário ativo no sistema de autenticação (Active Directory, por exemplo). Na base AD do PRODERJ, foi feito o somatório dos usuários ativos pertencentes a própria Autarquia, mais os usuários da base da Secretaria de Estado de Transformação Digital, órgão vinculado que compartilha a mesma estrutura física. O resultado deste somatório foram 632 usuários ativos. Nos prints abaixo, são apresentadas as bases do PRODERJ.





IV - **Item 4:** se faz necessário 1 (uma) unidade para cada usuário. Este item não existia no processo anterior, mas sua métrica e quantitativo são iguais às do item 3, ou seja, 632 usuários ativos;

V - **Itens 5, 6, 7 e 8**: se fazem necessárias 6 (seis) turmas, cada uma para 2 (dois) alunos. Este quantitativo leva em conta as duas diretorias que estarão envolvidas na implementação e operação da solução. A quantidade de turmas visa difundir o conhecimento para o máximo de servidores, incluindo funcionários de diferentes gerências e diretorias, compondo equipe de agentes multiplicadores, bem como resguardar eventual necessidade de novos treinamentos em razão de desligamento de servidores treinados.

VI - Diante das quantidades de licenças necessárias ao PRODERJ, foram acrescidos mais 20% ao quantitativo de licenças nos itens 1 ao 4, de modo a suprir um possível aumento no quadro de funcionários, estações de trabalho e/ou servidores, observada a lógica do Sistema de Registro de Preços.

VII - As demandas de treinamentos para o PRODERJ considerou a possibilidade de treinamento/capacitação de 6 técnicos dos quadros do PRODERJ, consideradas duas vagas para cada uma das três diretorias técnicas (Diretoria de Infraestrutura, Diretoria de Sistema e Soluções e Diretoria de Segurança da Informação). As duas vagas por diretoria viabilizará a capacitação de um colaborador técnico mais um suplente. A quantidade apontada busca também, dentro da lógica de SRP, resguardar eventuais desligamentos ou afastamentos prolongados de técnicos que já tenham sido treinados, de forma que sempre permaneça alguém com a capacitação adquirida na solução tecnológica tratada neste estudo.

9.2.2. Usuário corresponde a qualquer perfil de acesso ao sistema PRODERJ utilizado por funcionários, estagiários, terceirizados e colaboradores em geral que necessitem de acesso para o desempenho de suas funções ou cumprimentos de objetos contratados.

10. ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO

10.1. Na tabela abaixo uma estimativa de preços, com base em processos com objetos similares demonstrados na tabela do tópico 6 deste documento. Em etapas posteriores se realizará a cotação oficial dos preços para o presente objeto.

10.2. Saliente-se, em observação do item 8.2 da Nota Técnica nº 6/2023 do Egrégio Tribunal de Contas do Estado do Rio de Janeiro, no que se refere ao art. 8º da Instrução Normativa SEGES/ME nº 65/2021, que não foi localizado, dentre os catálogos de soluções de TIC com condições padronizadas publicados pelo Governo Federal, nenhum referente à solução "Plataforma de Gerenciamento de Identidades e Acessos" ou similar que pudesse ser utilizado o preço de referência.

10.3. Na análise das atuais práticas de mercado para ferramentas de gestão de identidades, constata-se que a modalidade “aquisição perpétua” não vem sendo opção para a contratação deste tipo de solução, com avanço de contratações via subscrição da ferramenta por períodos predefinidos (12, 24 ou 36 meses), bem como a opção pelo serviço gerenciado, ou ainda o uso de ferramentas open source.

10.4. Tal observação corrobora situação observada no Pregão PERP09/2023 que o PRODERJ promoveu no âmbito do SEI-150016/000766/2022, em que as empresas classificadas para o Lote 2 cujo objeto previa o fornecimento de licenças perpétuas para solução de gestão de identidades, acabaram desabilitadas por oferecerem tão somente a solução em modo SaaS (subscrição de licença

temporária).

10.5. Na tabela abaixo constam processos recentes cujo objeto trata de subscrição para solução de gestão de identidades, observados na Consulta de Licitações do Portal da Transparência:

Fonte	período de referência	Proteção Servidor - IAM (item 1)	Proteção Desktop IAM (item 2)	MFA (item 3)	Logon único (item 4)	Treinamento por turma (itens 5)	Treinamento por turma (itens 6)	Treinamento por turma (iten7)	Treinamento por turma (itens 8)
Prefeitura Municipal de Anápolis - GO - P.E. nº 10/2023	12 meses	R$ 945,00	R$ 489,00	R$ 266,00	R$ 395,00	não demandado	não demandado	não demandado	não demandado
Serviço Nacional de Aprendizagem do Cooperativismo - SESCOOP P.E. nº 6/2022	36 meses*	R$ 3.172,18	R$ 1.268,81	não demandado	não demandado	R$ 19.296,50**	R$19.296,50**	R$19.296,50**	R$19.296,50**
Tribunal Regional Eleitoral do Paraná - TRE/PR - P.E. nº 63/2022	36 meses*	não demandado	R$ 529.46	R$ 726,81	não demandado	não demandado	não demandado	não demandado	não demandado
Banco do Estado do Pará - BANPARÁ - P.E. nº 28/2023	48 meses*	R$ 1.761,68	R$ 720,40	não demandado	não demandado	não demandado	não demandado	não demandado	não demandado
Média da ordem de grandeza		**R$ 814,27**	**R$ 317,14**	**R$254,14**	**R$395,00**	**R$19.296,50**	**R$19.296,50**	**R$19.296,50**	**R$19.296,50**
Valor total p/item estimado contrato PRODERJ* **		**R$ 1.722.995,32**	**R$ 171.255,60**	**R$ 192.638,12**	**R$ 299.410,00**	**R$ 115.779,00**	**R$ 115.779,00**	**R$ 115.779,00**	**R$ 115.779,00**
Valor total estimado do contrato PRODERJ* **									**R$ 2.849.415,04**
* itens considerados em proporcionalidade ao período de 12 (doze) meses ** considerada turam para 2 pessoas *** consideradas as quantidades estimadas informadas na tabela do subtópico 9.1 deste documento									

11. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

11.1. A “Solução 1” (Open Source), ainda que sirva para suprir situações de emergência e apresente vantajosidade econômica por sua natureza open source (gratuita), via de regra, não é a mais adequada para implementação em ambientes corporativos, pois não oferece os níveis de atendimento de suporte técnico necessários para garantir o funcionamento adequado da solução, bem como o atendimento das necessidades de negócio, que exigem responsabilização e pronto restabelecimento em caso de falhas.

11.2. A “Solução 2” (Contratação da solução de Gerenciamento de Identidades no modelo Pay-as-you-go (Pague pelo uso)), mesmo sendo uma opção mais flexível do ponto de vista operacional e orçamentário, é limitado a um ambiente nuvem, ou seja, todas os acessos devem ser dentro da nuvem do provedor, o que não é a realidade do PRODERJ, que possui sistemas posicionados na infraestrutura interna do órgão.

11.3. A “Solução 3” (Contratação de solução de Gerenciamento de Identidade por Serviço Gerenciado), ainda que seja operacionalmente mais cômoda pelo fato da CONTRATADA ter a obrigação de manter e operar a ferramenta, apresenta um custo muito mais expressivo do que a simples subscrição. É também a opção mais cara, tanto pelo tipo de serviço prestado, quanto pelas ferramentas inclusas necessárias para a realização do objetivo da contratação. Por fim, a comodidade do serviço gerenciado pode não compensar o custo extra.

11.4. Nesse passo, entende-se que a “Solução 4” (Serviço de Subscrição) é a mais adequada para o atendimento da demanda atual do PRODERJ, pois a solução contratada possibilitará o gerenciamento centralizado da solução, bem como suprirá adequadamente a questão do suporte técnico por toda a vigência contratual da solução, enquanto a passagem de conhecimento ocorrerá por conta dos treinamentos.

11.5. Quanto ao modelo adotado para o serviço de treinamento, uma vez que não foi possível a observação no mercado de opções de treinamento por aluno/vaga e considerando as vantagens e possibilidade de mititação das desvantagens observadas, opta-se pelo formato de treinamento por turma (2 alunos).

12. DESCRIÇÃO DA SOLUÇÃO DE TI COMO UM TODO

Registro de Preços para a prestação de serviços de subscrição de Plataforma para Gerenciamento de Identidades, incluindo suporte técnico e treinamento, pelo período de 12 (doze) meses.

13. NATUREZA DO OBJETO DA CONTRATAÇÃO

13.1. Os itens que integram o objeto possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos. Portanto, se enquadram como SERVIÇOS COMUNS ou usuais de mercado, na forma do parágrafo único, do art. 6º, XIII, da Lei nº 14.133/2021.

13.2. O Objeto se constitui por soluções de TIC reunidas em lote único, observados os seguintes aspectos:

a) Os itens 1 a 4 do lote único são medidos em unidades e correspondem a serviços de subscrição de software (cada unidade corresponde a uma ANUIDADE de licença de software), com natureza contínua;

b) Os itens 5 a 8 do lote único são medidos por turmas (2 alunos) e correspondem a serviços de treinamento sob demanda, de natureza contínua.

13.3. **Critério de julgamento**

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, em SISTEMA DE REGISTRO DE PREÇOS, com adoção do critério de julgamento pelo MENOR PREÇO global, em observação do Art. 33, inciso I, da Lei nº 14.133/2021.

14. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

14.1. O agrupamento de itens em lote único proposto no presente estudo resguarda as características do objeto enquanto solução tecnológica única composta de quatro itens interdependentes, quais sejam os softwares previstos nos itens 1 a 4 do lote único(solução principal), bem como os respectivos serviços de treinamento e capacitação. O parcelamento do objeto entre fabricantes distintos não se aplica, em razão da correlação intrínseca entre os itens previstos do lote único.

14.2. O §3º, inciso II, do art. 40, da Lei nº 14.133/2021 resguarda a não adoção do parcelamento, como medida excepcional, quando o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido.

14.3. Uma solução integrada de gestão de identidades e acessos é projetada para funcionar de maneira coesa, com módulos e componentes que interagem entre si de forma harmoniosa. Quando essa solução é parcelada, ou seja, adquirida em partes separadas por meio de diferentes licitações ou contratos, há um risco significativo de incompatibilidade entre os componentes, falhas de integração e, consequentemente, vulnerabilidades de segurança.

14.4. Além disso, o parcelamento pode levar à fragmentação da responsabilidade técnica, dificultando a identificação de falhas e a implementação de correções. Isso pode resultar em custos adicionais para a administração pública, já que a integração de sistemas incompatíveis ou a correção de problemas decorrentes do parcelamento pode demandar investimentos extras em consultoria, desenvolvimento e manutenção.

14.5. O modelo resguarda o ganho de economia em escala, sem prejuízo a ampla competitividade, uma vez que existem no mercado várias empresas com capacidade de fornecer os produtos e serviços na forma em que estão agrupados neste estudo, bem como para facilitar a execução e fiscalização do contrato, propiciando maior nível de controle pela Administração, sendo prática comum reconhecida pelo mercado.

14.6. Assim, o parcelamento do objeto não é técnica e economicamente indicado, tendo em vista a preservação da harmonia entre todos os elementos da solução, bem como a total interoperabilidade dos componentes e a facilidade de uso e operação. Recomenda-se que a solução seja fornecida por um único fabricante, em que seus componentes, módulos e/ou programas estejam totalmente integrados.

15. RESULTADOS PRETENDIDOS

A presente demanda, em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis, visa a mitigação de ameaças de segurança cibernética que afetam a rede governo, bem como obter os seguintes benefícios:

a) Melhorar o controle de acesso para pessoas, processos e aplicativos;

b) Aumentar a resiliência do PRODERJ contra aqueles ataques cujo foco seja o roubo de identidade de usuários por meio de phishing;

c) Ampliar a auditabilidade das ações das credenciais de funcionários e colaboradores;

d) Ampliar a aderência com os padrões de segurança estabelecidos e regulamentos de conformidade.

e) Elevar a segurança dos serviços prestados aos cidadãos, por meio de ações de segurança da informação no âmbito da

f) Administração Pública;

g) Contribuir para a garantia da confidencialidade, integridade e disponibilidade das informações produzidas e armazenadas em meios tecnológicos no âmbito do Governo do Estado do Rio de Janeiro.

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

Não se vislumbra providências a serem adotadas que sejam antecedentes e necessárias à celebração de contrato para o objeto previsto neste documento.

17. REQUISITOS DE QUALIFICAÇÃO TÉCNICA

17.1. Comprovação de aptidão para a prestação de serviços de acordo com as características, quantidades e prazos compatíveis com o objeto, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, na seguinte forma:

I - Comprovação da experiência mínima de 12 (doze) meses e entrega de 10% (dez por cento) na execução do objeto, sendo aceito o somatório de atestados de períodos diferentes, não havendo obrigatoriedade de os 12 meses serem ininterruptos.

- Prova de atendimento aos requisitos de quantidade mínima de 10% (dez por cento), previstos na Lei Federal nº 14.133/2021, art. 67, §2º.
- Prova de atendimento aos requisitos de cumprimento de prazo mínimo de 12 (doze) meses, previstos na Lei Federal nº 14.133/2021, art. 67, §5º.

II - O(s) atestado(s) se aplicam aos itens 1 a 4 do lote único (serviços de subscrição de software), os quais correspondem à parcela de maior relevância ou de valor significativo para o objeto.

III - Um único atestado é suficiente para a demonstração da experiência anterior do licitante em relação a execução do objeto licitado, sendo admitida a soma de atestados ou certidões apresentados pelas licitantes, desde que tais documentos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

IV - O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

V - O(s) atestado(s) deverá(ão) referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

VI - Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços executados de forma concomitante, resultando na comprovação de capacidade técnico-operacional de uma única contratação.

VII - Em caso de dúvida fundada suscitada pelo pregoeiro, a Administração poderá solicitar ao licitante, em diligência complementar, todas as informações necessárias à comprovação da legitimidade dos atestados, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

17.2. A motivação para a comprovação de aptidão técnica, bem como os prazos e quantidades mínimas acima referido, se dá em virtude da realização do certame via Sistema de Registro de Preços com demanda em larga escala, para atendimento de inúmeros órgãos da Administração. Portanto, se faz razoável a verificação de que o futuro prestador do serviço tem capacidade de atendimento compatível com a criticidade do projeto, mitigando riscos à disponibilidade dos serviços do Governo, bem como diante da importância do objeto a ser contratado, que tem relação direta com a segurança institucional dos órgãos e secretarias do estado.

18. AMOSTRA, EXAME DE CONFORMIDADE E PROVA DE CONCEITO

Não se aplica a exigência prévia de amostra, exame de conformidade ou prova de conceito, para fins de adjudicação do objeto proposto neste estudo, tendo em vista que a análise da documentação técnica do produto a ser ofertado será suficiente para verificação quanto à aderência aos requisitos estabelecidos.

19. OBRIGAÇÕES DO CONTRATANTE E CONTRATADA

19.1. Obrigações da CONTRATANTE

a) Fornecer à Contratada documentos, informações e demais elementos que possuir pertinentes à execução do objeto.

19.2. Obrigações da CONTRATADA

a) A CONTRATADA deverá cumprir todas as obrigações constantes neste documento e em seus Anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

b) Indicar formalmente preposto apto a representá-lo junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

c) Assinar o Termo Confidencialidade e Sigilo, conforme o modelo a ser apresentado como anexo do futuro Termo de Referência;

d) deve disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.

e) Adicionalmente, deverá manter canal de atendimento por e-mail, telefônico e sistema web para a interação com o fabricante sempre que for necessário, e demais obrigações estabelecidas no presente documento, sem ônus para o CONTRATANTE.

19.3. As disposições nos subtópicos 19.1 e 19.2 correspondem às obrigações específicas relativas ao objeto delineado neste documento, ficando resguardadas todas as demais obrigações constantes do futuro Edital e da minuta do contrato a ele anexa.

20. ANÁLISE DA POSSIBILIDADE DE SUBCONTRATAÇÃO

20.1. Não será admitida a subcontratação, sub-rogação, cessão ou transferência no todo ou em parte, em razão da composição do objeto, constituído em lote único para o fornecimento de serviços especializados os quais configuram soluções tecnológicas interdependentes.

20.2. Saliente-se que, no caso do item de treinamento ser ministrado pelo mesmo fabricante da solução ofertada pela contratada ou com uso de sua plataforma, isso não configura subcontratação, sub-rogação, cessão ou transferência, uma vez que compõe a solução.

21. POSSIBILIDADE DE PARTICIPAÇÃO DE MICROEMPRESAS, PEQUENAS EMPRESAS E EMPRESAS INDIVIDUAIS

21.1. Não se aplica a reserva de cotas exclusivas para a participação de empresas constituídas em tais modalidades, tendo em vista que o objeto é constituído de itens distribuídos em lote único e indivisível, não podendo cada um ser licitado separadamente sem prejuízo do resultado ou da qualidade do serviço.

21.2. Ademais, o objeto apresenta valor estimado superior ao teto informado no art. 48, I da Lei Complementar nº 123/2006.

22. POSSIBILIDADE DE PARTICIPAÇÃO DE CONSÓRCIOS E COOPERATIVAS

22.1. Participação de empresas em regime de consórcio

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

22.1.2. A vedação se dá em razão das características específicas da solução a ser contratada, que não pressupõe multiplicidade ou heterogeneidade de atividades empresariais distintas, nem envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação definidos neste documento.

22.1.3. Entende-se que os itens a serem contratados não exigem empresas de diferentes segmentos e/ou capacidades reunidas para atuarem na execução do objeto proposto.

22.1.4. Ademais, a gestão compartilhada poderá gerar vícios ou lacunas no fluxo dos processos de atendimento. A cadeia de responsabilidades entre as empresas será maior que se o objeto estiver sob responsabilidade de uma única empresa, ainda que operacionalizado por meio de atuação conjunta com outras empresas.

22.1.5. Mesmo a garantia produzida como consequência da aquisição é resultado de equipes, técnicas e procedimento complementar, não havendo benefício ou necessidade de segmentação para a realização do objeto proposto, além de repercutir em vários canais de atendimento de eventuais chamados técnicos, gerando uma morosidade no atendimento e ocasionando o não cumprimento dos itens expostos neste documento e seus anexos.

22.1.6. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, 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 técnica. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

22.1.7. Tendo em vista que é prerrogativa do Poder Público, na condição de CONTRATANTE, a escolha da participação ou não de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme a literalidade do texto da Lei nº o 14.133, art 15 e seus incisos e parágrafos, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

22.1.8. Por fim, a vedação da participação de empresas reunidas em regime de consórcio visa exatamente afastar a restrição à competição, na medida em que a reunião de empresas que, individualmente, poderiam fornecer os equipamentos, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/cartéis para manipular os preços nas licitações.

22.2. Possibilidade de participação de cooperativas

22.2.1. Não se aplica a participação de cooperativas diante da especificidade do objeto, enquanto entrega de licenças de software por subscrição e seus respectivos cursos de treinamento, englobados em lote único, bem como observado o mercado de soluções para o objeto ora proposto, composto por empresas de organização tradicional aptas a fornecer a integralidade do objeto, não se faz razoável a participação de cooperativas neste certame

22.2.2. Ademais, a natureza dos serviços e o modo como serão executados, exige subordinação jurídica entre o contratante e o contratado.

22.2.3. Saliente-se, por fim, que os serviços tecnológicos do objeto proposto requer conhecimento técnico especializado na solução aplicada, não havendo no mercado cooperativa capaz de atender aos requisitos e padrões técnicos exigidos.

23. PRAZO DO CONTRATO E POSSIBILIDADE DE PRORROGAÇÃO

23.1. O prazo de vigência do contrato é de 12 (doze) meses, contado da data da divulgação no Portal Nacional de Contratações Públicas.

23.2. 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.

24. **LOCAL DE ENTREGA DOS BENS / PRESTAÇÃO DO SERVIÇO**

24.1. Resguardadas as formas de entrega descritas no subtópico 25.1 deste documento, os atendimentos de suporte técnico, quando eventualmente necessários por meio presencial e envio de técnico ao local, será realizada no endereço indicado pela CONTRATANTE.

24.2. No caso do PRODERJ, será em um dos três endereços abaixo, a definir na abertura do chamado:

a) Data Center – Universidade do Estado do Rio de Janeiro (UERJ). End.: R. São Francisco Xavier 524, 2º andar, bloco “F”, Maracanã, Rio de Janeiro – RJ, CEP: 20550-013;

b) Data Center – Centro Integrado de Comando e Controle (CICC). End.: Rua Carmo Neto s/nº, Cidade Nova, Rio de Janeiro – RJ - CEP 20210-051; ou

c) Sede – Centro de Tecnologia de Informação e Comunicação do Governo do Estado do Rio de Janeiro (PRODERJ). End.: R. da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011.

24.3. O acesso de representante da CONTRATADA nas dependências da CONTRATANTE, deverá ocorrer mediante prévia comunicação entre as partes, por meio dos mecanismos de comunicação definidos neste instrumento.

25. **PRAZOS E CONDIÇÕES DE ENTREGA DOS BENS E SERVIÇOS**

25.1. **Forma de Entrega**

25.1.1. A entrega dos serviços de subscrição (itens 1 a 4 do lote único), em parcela única e imediata, se dará de forma virtual, via liberação do acesso pela CONTRATANTE na plataforma da solução onde constará o total de licenças contratadas.

25.1.2. A entrega dos serviços de treinamento (itens 5 a 8 do lote único), em parcelas sob demanda, acontecerá através do portal de treinamentos da contratada ou que esta venha a disponibilizar.

25.2. **Prazo de Entrega**

O cronograma para as entregas do objeto, contados em dias úteis, será conforme a tabela abaixo:

Prazo	Marco para contagem do prazo	Atividades	Responsável
15	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Realização da Reunião Kick off e emissão Ordem de Serviço para subscrições	CONTRATANTE e CONTRATADA
5	Realização da reunião Kick off e emissão da Ordem de Serviço para subscrições	Liberação do acesso	CONTRATADA
20	Emissão da Ordem de Serviço para treinamento	Início do treinamento	CONTRATADA
15	Realização da reunião Kick off	Instalação dos agentes da solução nos ativos tecnológicos que foram indicados pela CONTRATANTE na reunião Kick off	CONTRATADA
30	Realização da reunião Kick off	Conclusão da configuração do escopo inicial de monitoramento na solução (entrega definitiva)	CONTRATADA
2	Recebimento do Relatório de Cumprimento do Objeto, previsto no subtópico 27.1, inciso II deste documento	Emissão do Termo de Recebimento Provisório	CONTRATANTE
20	Emissão do Termo de Recebimento Provisório	Emissão do Termo de Recebimento Definitivo / Autorização para emissão de Nota Fiscal / Fatura	CONTRATANTE

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

26.1. **Acordo de Nível de Serviço**

26.1.1. **Para os serviços de subscrição (itens 1 a 4 do lote único)**

I - **Finalidade:** Garantir a qualidade dos Serviços de subscrição.

II - **Periodicidade:** Trimestral

III - **Início da medição:** Após a emissão do Termo de Recebimento Definitivo.

IV - **Mecanismo de cálculo:** Na forma da tabela do subtópico 4.9.4.6 deste documento.

26.1.2. **Para os serviços de treinamento (itens 5 a 8 do lote único)**

I - **Finalidade:** Garantir a qualidade dos Serviços de Treinamentos.

II - **Periodicidade:** eventual, ao final do treinamento contratado, para fins de ateste de Nota Fiscal e emissão do Termo de Recebimento Definitivo

III - **Início da medição:** Após a emissão do Termo de Recebimento Definitivo.

IV - **Mecanismo de cálculo:** Os servidores participantes farão avaliação do curso com atribuição de grau, conforme os percentuais indicados abaixo:

a) I (insatisfatório) – 0 a 25%;

b) R (regular) – 26 a 50%;

c) B (bom) – 51 a 75%;

d) MB (muito bom) – 76 a 100%.

26.1.3. **Penalidades**

26.1.3.1. Ocorrerá aplicação de multa por motivo de descumprimento de nível de serviço exigido, conforme valores a seguir:

I - **Para os serviços de subscrição (itens 1 a 4 do lote único)**

a) 0,05% no valor do item correspondente, por demanda com severidade categorizada como "baixa" não atendida no prazo;

b) 0,15% no valor do item correspondente, por demanda com severidade categorizada como "média" não atendida no prazo;

c) 0,25% no valor do item correspondente, por demanda com severidade categorizada como “média alta” não atendida no prazo;

d) 0,40% no valor do item correspondente, por demanda com severidade categorizada como “alta” não atendida no prazo;

e) 0,40% no valor do item correspondente do mês de referência, por hora de indisponibilidade (total ou parcial), após o vencimento dos prazos para início e conclusão da demanda categorizada como "alta", até o limite de 8 horas.

II - **Para o serviço de treinamento (itens 5 a 8 do lote único)**

a) A Comissão de Fiscalização de Contrato atestará a Nota Fiscal do treinamento realizado, sem aplicação de multa, se no mínimo 60% das avaliações indicarem os graus B (bom) e/ou MB (muito bom).

b) A Comissão de Fiscalização de Contrato poderá aplicar alternativamente multa de até 2% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau R (regular).

c) A Comissão de Fiscalização de Contrato poderá aplicar alternativamente multa de até 5% sobre o valor da Nota Fiscal se 50% das avaliações indicarem o grau I (insatisfatório).

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

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

26.1.3.4. As multas por não cumprimento dos níveis de serviço serão descontadas da garantia de contrato prevista no subtópico 29 deste documento, resguardado o limite da mesma.

26.1.3.5. A Comissão de Fiscalização do Contrato deverá comunicar a Contratada, o resultado da apuração de multa, procedendo as tratativas em processo apartado, resguardada a ampla defesa e o contraditório.

26.1.3.6. 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.

26.1.3.7. Ficam resguardadas todas as demais sanções administrativas previstas na Lei de Licitações e Contratos.

26.1.3.8. Todas as solicitações de suporte técnico devem ser registradas pela contratada para acompanhamento e controle da execução do serviço.

26.1.3.9. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução. Para esses problemas a contratada deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução paliativa e informar ao CONTRATANTE, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada ao CONTRATANTE.

26.1.3.10. A contratada deverá, sempre que solicitado, emitir relatórios de atendimento de todas as intervenções realizadas, preventivas ou corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções.

26.2. **Modelo de gestão do contrato e fiscalizada pelo órgão ou entidade contratante**

26.2.1. A execução do contrato será acompanhada e fiscalizada por Comissão de Fiscalização de Contrato, composta na forma do Decreto Estadual nº 48.817/2023.

26.2.2. A CONTRATADA deverá designar e manter preposto, em suas próprias dependências, que deverá se reportar diretamente à Comissão de Fiscalização de Contrato, para acompanhar e se responsabilizar pela execução do contrato, inclusive pela regularidade técnica e disciplinar da atuação de equipe técnica eventualmente disponibilizada para o cumprimento do objeto.

27. **REGRAS PARA O RECEBIMENTO PROVISÓRIO E DEFINITIVO E CRITÉRIOS DE MEDIÇÃO**

27.1. O recebimento provisório do objeto, nos termos do art. 140, incisos I e II da Lei Federal nº 14.133/21, será realizado pela Comissão de Fiscalização do Contrato da CONTRATANTE na forma abaixo indicada:

I - Para todos os serviços previstos no lote único do objeto o recebimento ocorrerá mediante termo, no prazo máximo de 2 (dois) dias úteis a contar da entrega do Relatório de Cumprimento do Objeto abaixo referido;

II - A CONTRATADA deverá elaborar um Relatório de Cumprimento do Objeto (modelo a compor anexo do futuro Termo de Referência) a ser entregue à Comissão de Fiscalização de Contrato, que deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução dos itens entregues. O relatório deverá estar acompanhado, conforme o serviço entregue, das seguintes informações e/ou documentos:

a) Para os serviços dos itens 1 a 4 do lote único do objeto: documentação de evidência que comprove o licenciamento da solução contratada, tais como número de séries ou chaves de acesso; as informações para o acionamento do suporte técnico e também os documentos oficiais do fabricante e documentação da solução; e

b) Para os serviços dos itens 5 a 8 do lote único do objeto: certificados dos alunos treinados.

27.2. Após a emissão do Termo de Recebimento Provisório, a CONTRATANTE, por meio de sua Comissão de Fiscalização de Contrato, analisará a documentação entregue e poderá fazer inspeções ou promover diligências internas quanto às etapas executadas para a entrega do objeto, com a finalidade de verificar a adequação no seu cumprimento pela contratada, bem como verificar a necessidade de arremates, retoques e revisões finais que eventualmente se fizerem necessários.

27.3. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não proceder ao Termo de Recebimento Definitivo até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas na fase do recebimento provisório.

27.4. O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com os futuros 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.

27.5. Estando tudo em conformidade, será efetuado o recebimento definitivo mediante termo.

27.6. O recebimento definitivo do objeto será efetuado pela Comissão de Fiscalização do Contrato, nos termos do art.140, incisos I e II da Lei Federal nº 14.133/2021, no prazo máximo de 20 (vinte) dias úteis, depois da emissão do Termo de Recebimento Provisório.

27.7. Com o recebimento definitivo, que concretiza o ateste do cumprimento do objeto contratado, a CONTRATANTE comunicará à CONTRATADA para que, em até 5 dias, emita a Nota Fiscal ou Fatura.

27.8. A Comissão de Fiscalização de Contrato, sob pena de responsabilidade administrativa, anotará em registro próprio as ocorrências relativas à execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 10 (dez) dias, para ratificação.

27.9. A CONTRATADA declarará, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a lhes fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem julgados necessários ao desempenho de suas atividades.

27.10. A instituição e a atuação da fiscalização do objeto do contrato não exclui ou atenua a responsabilidade da CONTRATADA, nem a exime de manter fiscalização própria.

28. **CRITÉRIOS DE MEDIÇÃO, DE PAGAMENTO E FORMA DE REAJUSTAMENTO DO CONTRATO**

28.1. **Forma e prazo de pagamento**

28.1.1. **Para os itens 1 a 4 do lote único**

A CONTRATANTE deverá pagar o preço ao CONTRATADO em parcela única, na conta-corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro.

28.1.2. **Para os itens 5 a 8 do lote único**

A CONTRATANTE deverá pagar o preço ao CONTRATADO em parcela sob demanda, na conta-corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro.

28.1.3. 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.

28.1.4. 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 48.817/2023.

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

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

28.1.7. Recebida a Nota Fiscal ou Fatura, 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, observadas as abrangências de aplicação por consulta aos seguintes cadastros:

1. SICAF;
2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis);
3. Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php);
4. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep);
5. Lista de inidôneos mantida pelo Tribunal de Contas da União; e
6. Módulo Registro de Ocorrências do SIGA;

c) por consulta ao SICAF, eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

28.1.8. 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.

28.1.9. 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.

28.1.10. 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.

28.1.11. 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.

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

28.1.13. 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.

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

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

28.1.16. 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.

28.1.17. 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 Índice Nacional de Preços ao Consumidor Amplo Especial (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.

28.1.18. 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.

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

28.2. **Reajuste de preços**

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

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

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

28.2.4. Os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA.

- A adoção do ICTI busca melhor equilíbrio contratual na medida em que é índice específico para soluções tecnológicas. Trata-se de índice mais equilibrado em relação aos índices de preços gerais, uma vez que os custos efetivos de TIC evoluem de forma diferente da média dos preços na economia.

28.2.5. No caso de atraso ou não divulgação do(s) índice(s) de reajustamento, a 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).

28.2.6. 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.

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

28.2.8. 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.

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

28.2.10. 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.

28.2.11. 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.

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

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

28.2.14. 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.

29. **CONDIÇÕES DE GARANTIA CONTRATUAL**

29.1. O Contrato conta com garantia de execução, nos moldes do artigo 96 da Lei nº 14.133/2021, correspondente a 5% (cinco por cento) de seu valor anual.

- O referido percentual, resguardada a discricionariedade prevista no citado art. 96, caput e o teto estabelecido no caput do art. 98 do mesmo diploma legal, considera a natureza do objeto, enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do órgão contratante em razão das exigências trazidas pela nova legislação quanto ao tratamento de dados pessoais.

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

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

b) seguro-garantia;

c) fiança bancária; e

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

29.3. 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 nele 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.

29.4. 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.

29.5. 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.

29.6. Ressalvada a hipótese de seguro-garantia, o CONTRATADO apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério da CONTRATANTE, contado da assinatura do Contrato, o comprovante de prestação de garantia, na forma do item 29.2.

29.7. 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 29.5 deste documento; e

d) a apólice somente será aceita se contemplar todos os eventos indicados no item 29.3, observada a legislação que rege a matéria.

29.8. 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.

29.9. 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.

29.10. Caso a opção seja por garantia em dinheiro, deverá ser efetuada em favor da CONTRATANTE, na conta-corrente da instituição financeira contratada pelo Estado, cujo valor será corrigido monetariamente e restituído ao CONTRATADO, na forma do item 29.16.

29.11. 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 29.1 neste item.

29.12. 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.

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

29.13. A CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

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

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

29.15. 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.

29.16. 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.

29.16.1. 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.

29.17. O CONTRATADO autoriza a CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista.

30. **POSICIONAMENTO CONCLUSIVO**

30.1. O presente ETP, bem como os seus anexos, consideram a necessidade de contratação dos serviços previstos neste objeto, os requisitos técnicos, legais, ambientais e os do próprio negócio, o mercado em que o objeto se encontra inserido, bem como os demais requisitos necessários para a caracterização e quantificação da demanda identificada, bem como o processo de escolha da solução que melhor se adéqua à Instituição nesta oportunidade.

30.2. São 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

30.3. O objeto ora proposto é medida que, no caso concreto, aumenta a competição, é a opção mais vantajosa e, ainda, mais condizente com o interesse público.

30.4. Resguardadas as considerações nos subtópicos 2.2 e 2.3 deste documento, não há risco de sobreposição com outras contratações existentes no PRODERJ.

30.5. 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.

31. CLASSIFICAÇÃO DESTE DOCUMENTO QUANTO AO GRAU E PRAZO DE SIGILO

Observadas as disposições da Lei Federal nº 12.527/2011 e do Decreto Estadual nº 46.475/2018, que tratam do direito e das restrições de acesso às informações sob guarda do poder público, fica registrado que o presente documento, assim como os seus anexos, são de acesso PÚBLICO.

32. ANEXOS

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 (98839100);

II - Mapa de Riscos (98839125);

III - Orientação para preenchimento do IRP (98839138).

33. ASSINATURA DOS MEMBROS DA EQUIPE RESPONSÁVEL PELO ESTUDO

Monique Gonçalves Paz Diretora de Segurança da Informação ID nº 4349648-2	Rosana Alves de Andrade Gerente de Proteção de Dados e Sistemas ID nº 4347470-5	Charles Monteiro Guimarães Diretor de Patrimônio e Logística ID nº 4432892-3	Marco Antônio de Andrade Assessor-chefe da Vice-Presidência de Administração ID nº 4284601-3

Rio de Janeiro, 27 de abril de 2025

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 28/04/2025, às 17:19, 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 28/04/2025, às 17:27, 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 **Monique Goncalves Paz**, **Diretora**, em 28/04/2025, às 18:01, 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 **Rosana Alves de Andrade**, **Analista de Sistemas**, em 28/04/2025, às 18:21, 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 **98839494** e o código CRC **B1D9A472**.

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

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 ESTUDO TÉCNICO PRELIMINAR

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

- Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar do qual é parte integrante e indissociável.
- O lote único com os itens componentes do objeto se encontram nas tabelas dos subtópicos 9.1. do Estudo Técnico Preliminar.

1. ESPECIFICAÇÕES TÉCNICAS

1.1. Proteção local e elevação de privilégios em servidores (item 1):

1.1.1. A solução deverá garantir a segurança para identidades e acessos para servidores com sistemas operacionais Microsoft Windows e Linux.

1.1.2. **Requisitos mínimos aplicados a Servidores Windows:**

1.1.2.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;

1.1.2.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino;

1.1.2.3. Oferecer opções de execução sem aviso: de aplicações com privilégios em modo explícito e transparente, monitorada de aplicações em modo explícito e transparente, com restrições de aplicações em modo explícito e transparente;

1.1.2.4. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa;

1.1.2.5. Disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

1.1.2.6. Suportar, no mínimo, os seguintes sistemas operacionais: Windows Server 2012/2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022;

1.1.2.7. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;

1.1.2.8. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via monitores/gravadores de acessos ou diretamente no ativo;

1.1.2.9. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;

1.1.2.10. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

1.1.2.11. Permitir a criação de políticas reutilizáveis, contendo, no mínimo, os seguintes tipos de aplicações ou tipos de arquivos: executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX, objetos COM;

1.1.2.12. Permitir a verificação do hash do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;

1.1.2.13. Suportar ao nome exato da aplicação / arquivo / script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;

1.1.2.14. Utilizar eventos reportados na interface da solução para criação de novas políticas ou incluí- los em políticas existentes;

1.1.2.15. Permitir agrupar aplicações com base em suas características, para facilitar a inserção de novas aplicações aos grupos ou políticas de segurança de aplicações já criadas;

1.1.2.16. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da console de gerência;

1.1.2.17. Disponibilizar o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;

1.1.2.18. Monitorar e exibir acessos e atividades realizadas na própria solução;

1.1.2.19. Permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;

1.1.2.20. Realizar varreduras utilizando as funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes;

1.1.2.21. Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional alvo;

1.1.2.22. Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;

1.1.2.23. Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;

1.1.2.24. Oferecer monitoramento ou detecção quanto a tentativas de roubo de credenciais;

1.1.2.25. Caso o dispositivo não possa estar conectado de forma permanente aos monitores/gravadores de acessos da solução e repositório seguro de credenciais, deve, de forma autônoma e off-line, gerenciar as senhas das credenciais locais, aplicando políticas de randomização e sincronização das senhas definidas na central da solução;

1.1.2.26. Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados;

1.1.2.27. Permitir criar uma whitelist para execução de aplicativos confiáveis, onde qualquer outra aplicação fora desta lista automaticamente seja bloqueada;

1.1.2.28. Possuir uma integração com Windows UAC, e conter relatórios do uso de prompts aos usuários feitos pelo UAC;

1.1.2.29. Suportar a guarda de políticas de hosts que não fazem parte do Active Directory;

1.1.2.30. Possuir cache de políticas aplicadas no endpoint, permitindo a segurança dos endpoints, ainda que ele não esteja conectado à rede corporativa;

1.1.2.31. Permitir que mensagens customizadas sejam apresentadas antes que uma aplicação seja executada ou bloqueada;

1.1.2.32. Deve suportar adição múltiplas mensagens, estas mensagens devem possibilitar edição e suportar múltiplas linguagens;

1.1.2.33. Deve possuir capacidade de gerar relatórios de aplicações e eventos de usuários inclusos na solução;

1.1.2.34. Realizar varredura e inventário de aplicações instaladas no sistema operacional.

1.1.3. **Requisitos mínimos aplicados Servidores Linux:**

1.1.3.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;

1.1.3.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino fazendo uso de agente instalado no sistema ou método análogo;

1.1.3.3. Suportar, no mínimo, os seguintes sistemas operacionais: Debian, Redhat Linux 7.x (64- bit), Redhat Linux 8.x (64-bit);

1.1.3.4. Disponibilizar, como conjunto mínimo de atividades controladas no ativo de destino, as seguintes operações: criação e exclusão de arquivos e diretórios, mudança de nome de arquivos e diretórios, abertura de arquivos para escrita, comandos chown e chmod e ligações entre arquivos;

1.1.3.5. Implementar restrições, em uma plataforma, de maneira global ou em uma conta de usuário ou grupo de maneira granular;

1.1.3.6. Realizar o controle mediante interceptação do comando antes que ele seja executado;

1.1.3.7. Permitir a liberação de comandos privilegiados a usuários comuns;

1.1.3.8. Permitir que os comandos executados em sistemas monitorados sejam gravados em modo texto no repositório seguro digital;

1.1.3.9. Permitir que sejam atribuídas permissões para usuários e grupos, inclusive do Active Directory;

1.1.3.10. Permitir o agrupamento de comandos, bem como a utilização de coringas como (*), para uma definição ampla de parâmetros;

1.1.3.11. A solução deverá possuir funcionalidade que permita definir variáveis de ambiente no momento da execução de um comando, independente da definição realizada pelo usuário ou seu perfil. Sendo exigido no mínimo as seguintes variáveis: PATH, ENV, BASH_ENV, GLOBIGNORE, SHELLOPTS;

1.1.3.12. Possibilitar o uso da máscara de usuário na execução dos comandos (valores entre 0000 e 0777);

1.1.3.13. Impedir a utilização da técnica de ShellEscape, em que um programa autorizado e executado com privilégios permita a execução de outros programas e consequentemente escape dos controles definidos;

1.1.3.14. Disponibilizar a funcionalidade de restrição de Shell, que impossibilite que scripts e shells de sistema executem comandos não permitidos pelas regras definidas na solução;

1.1.3.15. Oferecer a capacidade de verificação da identidade da pessoa que executa comandos localmente no dispositivo alvo através de autenticação via usuário da ferramenta, LDAP ou RADIUS;

1.1.3.16. Monitorar e exibir acessos e atividades realizadas no próprio sistema;

1.1.3.17. Possibilitar mapear e coletar atividades regulares de usuários através do modo observação, agregando e exportando os resultados para um perfil;

1.1.3.18. Prover um controle de comandos completo, com a possibilidade de criar uma lista de comandos permitidos ou bloqueados (whitelisting/blacklisting), a serem alterados (criação de alias) ou prevenir que comandos sejam executados ou permitir trabalhar em Shell modificado/controlado;

1.1.3.19. Prover meios de permitir que os usuários executem comandos específicos e conduzam sessões remotamente baseado em regras sem autenticar-se diretamente utilizando credenciais privilegiadas.

1.2. **Proteção local e elevação de privilégios em desktops (item 2)**

1.2.1. Prover as funcionalidades através de agentes instalados no sistema operacional e permitir a proteção e controle dos privilégios;

1.2.2. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente no servidor de destino;

1.2.3. Realizar varredura e inventário de aplicações instaladas na estação de trabalho;

1.2.4. Garantir o controle e bloqueio de comandos, mesmo que o acesso seja realizado diretamente na estação de trabalho de destino (sem ser através do Repositório Seguro), fazendo uso das funcionalidades instaladas no sistema operacional;

1.2.5. Oferecer opção de execução de aplicações com privilégios em modo explícito e transparente (sem avisos);

1.2.6. Oferecer opção de execução monitorada de aplicações em modo explícito e transparente (sem avisos);

1.2.7. Oferecer opção de execução com restrições de aplicações em modo explícito e transparente (sem avisos);

1.2.8. Exibir a reputação do arquivo executado advinda de, pelo menos, 1 (uma) fonte externa;

1.2.9. Disponibilizar a opção de encaminhamento de arquivo suspeito para análise de malware em soluções de mercado;

1.2.10. Suportar pelo menos as seguintes versões de estações de trabalho: Windows 10 x32 & x64, Windows 11 x64;

1.2.11. Implementar regras de controle de aplicações permitidas e bloqueadas para execução fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via Repositório Seguro ou diretamente no ativo;

1.2.12. Implementar regras de controle do nível de privilégio utilizado na execução das aplicações permitidas fazendo uso das funcionalidades instaladas no sistema operacional alvo, independentemente do acesso ao ativo ser realizado via mecanismo de Monitoramento Comportamental e Repositório Seguro ou diretamente no ativo;

1.2.13. Implementar controle de nível de privilégio independentemente da permissão que o usuário possua localmente no ativo ou no domínio, permitindo que usuários restritos executem atividades com nível administrativo;

1.2.14. Permitir atribuição granular para execução de aplicações com nível de privilégio administrativo, sem que esse privilégio seja global na máquina;

1.2.15. Permitir a criação de objetos reutilizáveis que possam conter no mínimo os seguintes tipos: arquivos executáveis, scripts, aplicações nativas Windows, bibliotecas dinâmicas (DLL), instaladores, controles ActiveX e objetos COM;

1.2.16. Implementar a verificação de hash do arquivo, dos parâmetros permitidos e da assinatura de fabricante, para objetos reutilizáveis da solução;

1.2.17. Implementar o suporte ao nome exato da aplicação/arquivo/script e expressões regulares em qualquer formato, para objetos reutilizáveis da solução;

1.2.18. Utilizar eventos reportados na interface da ferramenta para novas políticas ou incluí-los em políticas existentes;

1.2.19. Permitir agrupamento de características e aplicações para fácil seleção e inclusão em políticas de segurança;

1.2.20. Impedir a desativação das funcionalidades instaladas no sistema operacional alvo sem autorização e/ou registro da atividade por meio da interface de gerência;

1.2.21. Disponibilizar modo de observação, em que não há bloqueios, mas há o registro das execuções e atividades dos usuários, facilitando a criação de políticas baseadas em comportamento conhecido;

1.2.22. Monitorar e exibir acessos e atividades realizadas na própria solução.

1.3. **Autenticação multi-fator adaptativa (item 3)**

1.3.1. A solução deverá ser capaz de atender minimamente os seguintes casos de uso para requisitar um e mais fatores de autenticação:

I - Multi Fator de autenticação para soluções de VPN via RADIUS ou SAML.

II - Qualquer dispositivo ou sistema operacional que suporte RADIUS.

III - Plugin para ADFS (IDP, Identity Provider), Active Directory Federation Services.

IV - Sob demanda utilizando o protocolo Oauth e REST APIs.

V - Para realizar o autosserviço de reset de senha ou desbloqueio de usuário.

1.3.2. A solução deverá ser capaz de oferecer minimamente os seguintes métodos para múltiplo fator de autenticação:

I - Usuário e senha dos diretórios suportados na solução.

II - Através de aplicativo para dispositivos móveis do tipo IOS e Android, oferecendo suporte para:

a) Biometria do tipo FaceID.

b) Biometria através do leitor de digital.

c) Smartphone push (Notificação para aprovar ou recusar uma autenticação).

d) Geolocalização a banco de dados de IPs.

e) Suporte a tokens OATH OTP.

f) Autenticação na tela de login via QRcode sem a necessidade de digitar usuário e senha, com opção de forçar a biometria no dispositivo móvel.

g) Ligação telefônica requisitando um PIN previamente configurado.

h) Mensagem de texto via SMS oferecendo o código para entrada manual e também uma URL única presente na mensagem de texto que ofereça a opção de aprovar ou recusar a autenticação sem a necessidade de digitar o código manualmente.

i) Confirmação de código via email.

j) Clientes do tipo OATH OTP (exemplo, Google Authenticator).

k) Autenticadores que suportem FIDO2 / U2F, minimamente suportando: Windows Hello, Yubikey, Google Titan Key, MacOS TouchID e Perguntas e respostas previamente configuradas.

III - Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através do portal web da solução.

IV - Permitir que os usuários realizem o autosserviço de reset de senha e desbloqueio de usuário utilizando os métodos de múltiplo fator de autenticação citados para verificação positiva através de REST APIs oferecidas pela solução.

V - É desejável que a solução possibilite integrações e customizações através de SDK (Software Development Kits) para aplicações mobile. Estes SDKs não devem ter um custo adicional;

VI - Para cada caso de uso ou conjunto de casos de uso de múltiplo fator de autenticação citados, a solução de ser capaz de identificar os atributos de contexto de cada autenticação para disponibilizar os melhores métodos definidos para a autenticação, suportando minimamente:

a) Endereçamento IP.

b) Dia da Semana.

c) Datas específicas.

d) Janelas de tempo entre duas datas.

e) Janelas de tempo entre horários (exemplo, horário comercial).

f) Tipo do Sistema Operacional.

g) Tipo do Browser.

h) Perfis configurados na solução.

i) País que está sendo realizado o acesso.

j) Se é um dispositvo gerenciado.

k) Autenticação via certificado.

l) Nível de Risco da autenticação medido por um motor de análise de comportamento dos usuários.

VII - A solução deve ter a capacidade de verificar antes de realizar um login em uma aplicação se o endpoint gerenciado está em conformidade com a solução de gerenciamento de endpoint (Unified Endpoint Management - UEM), devendo suportar minimamente:

a) Microsoft Intune

b) VmWare Workspace Obe

c) JAMF

VIII - A solução deve ter capacidade de detectar casos de uso e perfis de autenticação já validados pelos usuários e não requisitar mais os mesmos durante um período de tempo configurado pelo administrador da solução, evitando desta forma repetidas validações em um curto espaço de tempo.

IX - O conjunto de fatores de autenticação disponibilizados devem ser baseados durante o acesso através de regras especificadas no item anterior e segregados por:

a) Conjunto de aplicações.

b) Um única aplicação.

c) Regras para o autosserviço de reset de senha e desbloqueio de usuário.

d) Portal do Administrador.

e) Portal do Usuário.

X - A solução deve prover um portal WEB para o usuário final;

XI - Permitir o usuário realizar o auto-registro de seus fatores de autenticação, tais como, perguntas e respostas, FIDO2 tokens, OATH OTP, definir PIN para chamada telefônica, TouchID, FaceID, Windows Hello, dentre outros.

XII - Permitir o usuário redirecionar autenticação multi-fator para outros usuários (desde que permitido).

XIII - Permitir os usuários gerenciarem seus dispositivos registrados, para Smartphones Android, IOS

XIV - Permitir aos usuários a capacidade de gestão para realizar o auto-registro de novos dispositivos móveis.

XV - Configurar OATH OTP para autenticação multi-fator nos sistemas operacionais Windows e MacOS (telas de login e bloqueio) quando os mesmo estão desconectados da internet com a finalidade de prover MFA mesmo quando sem internet para o sistema operacional.

XVI - A solução deve prover um aplicativo móvel para Android e IOS;

XVII - Permitir configurar OATH OTP adicionais provenientes de outras soluções.

XVIII - Deve verificar dispositivos registrados (dispositivos móveis e sistemas operacionais).

XIX - Deve ter integração nativa com FaceID, TouchID, leitor biométrico dos dispositivos móveis alavancando os mesmos para autentição biométrica durante login nas aplicações.

XX - Deve reportar coodernadas GPS para os sistemas que utilizam geolocalização.

XXI - Deve detectar ROOT em dispositivos Android e Jailbreak em dipositivos IOS com a finalidade de detectar atividades maliciosas e como consequência o aplicativo é desabilitado para uso

XXII - O aplicativo deve suportar autenticação do tipo push, onde o usuário tem a escolha de aceitar ou recusar o desafio, esta notificação de conter minimamente:

a) Data e Hora.

b) Cidade / Geolocalização do acesso

c) Aplicação sendo acessada.

XXIII - A solução deve possuir a capacidade de realizar o login sem a utilização da senha (passwordless) realizando o scan de QR code gerado na tela de login do portal de aplicação através do aplicativo móvel do fabricante, sem a necessidade inclusive de digitar o usuário a ser logado na aplicação. Deve adicionalmente ter a opção de forçar a utilização de biometria oferecida pelo smartphone / telefone celular.

XXIV - A solução deve possuir um aplicativo para Windows e MacOs com suporte a multifator de autenticação do tipo OTP (one time password) do próprio fabricante da solução de multifator. Este aplicativo dará suporte para casos onde não será possível o uso de um telefone celular / smartphone.

XXV - Permitir autorização de acesso às aplicações e arquivos, quando incluídos em regras, individualmente ou em grupos;

a) Deve realizar varreduras fazendo uso das funcionalidades instaladas no sistema operacional alvo para catalogar arquivos existentes nas máquinas e uni-los ao inventário populado mediante detecção durante a execução;

b) Deve verificar a reputação dos arquivos executados e detectados pelas funcionalidades instaladas no sistema operacional alvo ou mecanismos de controle de ameaças (VirusTotal.com ou similares);

c) Permitir a execução automática de tipos desconhecidos de arquivo, de acordo com sua origem, mesmo possuindo restrições;

XXVI - Possibilitar ao usuário final a solicitação de liberação de atividades específicas fazendo uso das funcionalidades instaladas no sistema operacional;

XXVII - Possibilitar a liberação emergencial da execução de comandos e elevação de privilégios sem desativar a solução, caso o usuário esteja off-line;

XXVIII - Implementar as regras de controle de acordo com características do usuário final, incluindo nome de usuário, grupos a que o usuário pertence e endereço IP;

XXIX - Permitir o envio de arquivos suspeitos, executados sob sua supervisão, para soluções de análise de ameaça do tipo Sandbox.

XXX - Possibilitar a execução de aplicativos que precisam de privilégio de execução a usuários não-privilegiados.

XXXI - Permitir a salvaguarda das contas privilegiadas em um único repositório seguro.

XXXII - A solução deve fornecer proteção de grupos de privilégios, o que significa que os usuários não podem adulterar ou modificar grupos privilegiados locais, como o grupo Administradores ou Power Users;

XXXIII - Solução deve automaticamente permitir os aplicativos de lista branca implantados por ferramentas de implantação de software por administradores confiáveis, incluindo o SCCM (Microsoft System Center Configuration Manager)

XXXIV - A solução deve permitir criar uma lista de aplicativos permitidos (allow list), onde seja possível configurar todos os aplicativos que podem ser executados e qualquer outra aplicação fora desta lista seja bloqueada automaticamente.

XXXV - Permitir criar uma lista branca (whitelist) de aplicativos, onde é configurado todos os aplicativos que podem ser executados, onde qualquer outra aplicação fora desta lista, seja automaticamente seja bloqueada;

XXXVI - A solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados para cálculo de risco.

XXXVII

- A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos:

a) Geo Velocidade, medindo velocidade de deslocamento do login, comparando a localização do último login com a atual, evitando “viagens impossíveis”, e traçando o comportamento do usuário neste quesito, por exemplo, pessoas que viajam muito podem ter uma pontuação de risco baixa mesmo que sua Geo Velocidade seja maior que pessoas que não viajam.

b) Geo Localização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual.

c) Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.

d) Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.

e) Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual.

f) Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual

g) O cálculo do risco pelo motor de aprendizado de máquina não utilize somente um atributo fora da normalidade reconhecida anteriormente pelo mesmo, mas sim em uma única autenticação calcule o risco baseado em todos os atributos citados acima e suas anormalidades em uma única autenticação. Exemplo, uma identidade tem por costume realizar sua autenticação as 9,10 e 11 da manhã, nas aplicações A e B, nas segundas-feiras e quintas-feiras, utilizando um dispositivo Android, das cidades de Brasília e São Paulo. Em futuro login acababa realizando a autenticação as 14 horas (fora do seu horário regular), na aplicação A, em um sábado (não é um dia da semana usual para esta identidade), de um dipositivo IOS (também não usual), da cidade de Brasília. O motor de aprendizado de máquina deve ter a capacidade de reconhecer estes três desvios de comportamento e retornar um risco calculado (alto, médio, baixo ou sem risco) referente a mesma.

XXXVIII

- A solução deverá prover múltiplo fator de autenticação para casos de uso com capacidade de interpretação de risco adaptativo baseados em algotimos de aprendizado de máquina e reconhecimento de comportamentos temporais para cada identidade (dias da semana e horários), o mesmo calculado antes da autenticação para tomada de ações antes da materialização da autenticação.

XXXIX

- Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias:

a) Sem risco

b) Risco Baixo

c) Risco Médio

d) Risco Alto

XL - Deve prover para os administradores da solução a personalização da influência na medição do risco para cada atributo citado neste item. Por exemplo, para a CONTRATANTE a geo velocidade pode ser um fator que não possui relevância, desta forma deve ser possível configurar a influência deste risco como baixa na modelagem de risco da plataforma;

XLI - O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação que realizam o login para os casos de uso citados neste documento e utilizar como contexto para:

a) Requisitar múltiplos fatores de autenticação de forma dinâmica.

b) Permitir o login sem o uso de múltiplos fatores.

c) Negar a autenticação.

XLII - Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.

XLIII - Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis

XLIV - Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores.

XLV - Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado, como, por exemplo, Palo Alto Cloud.

XLVI - Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo E-mail com conteúdo do alerta e Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack.

XLVII - Possuir dashboards pré-configurados com informações e gráficos com as seguintes caracteríticas:

a) Utilização do Motor de Análise do Comportamento dos Usuários.

b) Comportamento dos usuários na utilização das aplicações.

c) Visão sobre a segurança das aplicações.

d) Mapa com a geolocalização das autenticações.

e) Visão sobre o comportamento dos Endpoints (Mobile e Computadores).

f) Visão sobre o comportamento das Identidades.

XLVIII - A solução deve permitir a configuração de dashboards personalizados.

XLIX - Deve permitir o compartilhamento dos dashboards com outros usuários.

1.4. **Logon único adaptativo para identidades dos colaboradores (item 4)**

I - A solução deve prover um catálogo de aplicações Web com modelos de configuração de Single Sign-On (SSO) abrangendo as aplicações mais conhecidas de mercado, com a finalidade de facilitar a configuração destas integrações.

II - A solução deve permitir a configuração do SSO para aplicações Web minimamente através dos seguintes protocolos e métodos:

a) SAML 2.0

b) Oauth 2.0 modo client

c) WS-Federation

d) OpenID connect

e) NTLM

f) Oauth 2.0 modo server

g) HTTP Basic

III - Suportar SSO via IWA (Integrated Windows Authentication) o qual reutiliza o login de rede para autenticação nas aplicações web, sem a necessidade de digitar usuário e senha novamente.

IV - Oferecer suporte para a personalização das repostas SAML, como por exemplo, mapear atributos dos diretórios para atributos SAML, ter a capacidade de incluir lógicas complexas para manipulação das repostas SAML e possibilitar a visualização da reposta SAML configurada antes de sua implantação.

V - A solução deve prover um portal WEB para o usuário final com as seguintes características:

a) Depois de efetuado o login apresentar as aplicações WEB disponíveis para realizar o SSO, através de um conjunto de ícones onde cada um representa uma aplicação que o usuário tem o direito de efetuar o SSO;

b) Realizar mudanças em atributos da identidade, tais como, telefone celular, email e foto.

c) Verificar as atividades de sua identidade através de dashboard com as seguintes informações:

- A) Total de logons.
- B) Total de falhas de logon.
- C) Geolocalização dos seus logons.
- D) Verificar a Geolocalização atual de seus dispositivos registrados.
- E) Utilização das aplicações.
- F) Histórico de eventos importantes, tais como, nova aplicação adicionada em seu portal de SSO, falhas de logon, dentre outros.

VI - Deve possuir serviço de diretório para armazenar identidades na solução, sem a dependência da sincronização com outros serviços de diretório on-premisses ou na nuvem de terceiros.

VII - O serviço de diretório da solução deve ser auto-escalável para suportar um grande número de identidades e multiplas autenticações simultâneas.

VIII - Deve ter a capacidade de forçar a complexidade das senhas, minimamente para os seguintes requisitos:

a) Tamanho mínimo.

b) Tamanho máximo.

c) Requerer mínimo de dígitos.

d) Requerer letras maiúsculas e minúsculas.

e) Requerer caracter especial (símbolo).

f) Limitar caracteres consecutivos.

g) Forçar expiração de senhas baseadas na idade das mesmas.

h) Guardar histórico de senhas para evitar reutilização

IX - Prover notificação para expiração das senhas por email.

X - Capturar falhas de logon repetidas para bloqueio do usuário

XI - A solução deve suportar adicionalmente a integração com serviços de diretório On-premisses e em nuvem, suportando minimamente:

a) Microsoft Active Directory.

b) Microsoft Azure AD

c) Google Directory

d) Diretórios LDAP

XII - As integrações realizadas com diretório de terceiros não devem realizar sincronismo com estas bases, ou seja, carregar todo o diretório configurado para a nuvem, a solução deve atuar como um intermediário (“broker”) entre os serviços de diretório de terceiros e a solução.

XIII - A solução deve possuir integração com provedores de identidades sociais com a finalidade de delegar a autenticação para tais provedores e atender possíveis requisitos de negócio, suportando minimamente os seguintes provedores:

a) Google.

b) Facebook.

c) LinkedIn.

d) Microsoft.

XIV - A solução deve ter a capacidade de configurar IDPs (Identity Providers) de parceiros de negócio da CONTRATANTE para dar acesso às identidades federadas em aplicações de negócio da CONTRATANTE sem a necessidade de criação de uma nova identidade na infraestrutura, por meio de federação realizada através do protocolo SAML.

XV - A solução deve ter a capacidade de configurar um timeout por sessão e quantidade de sessões simultâneas, desta forma quando a sessão atingir tal tempo configurado de inatividade ou sessões simultâneas realizar o logout automático deste usuários nas aplicações conectadas.

XVI - O conector on premisses da solução que faz a comunicação do datacenter do cliente com a nuvem da solução SaaS deve ser único e sem a necessidade de instalação de componentes individuais para cada papel que o mesmo desempenhará, adicionalmente não deve depender de componentes de terceiros para ter alta disponibilidade e balanceamento de carga (exemplo, balanceadores de carga de terceiros). Em um único serviço ou agente on premisses deve englobar minimamente os seguintes componentes:

a) Servidor RADIUS

b) Cliente Radius

c) Proxy reverso

d) Integração com LDAP e Microsoft AD

e) IWA, Integrated Windows Authentication

XVII - A solução deve oferecer um componente/software para intermediar o SSO em aplicações Web sitiadas no datacenter da CONTRATANTE sem a necessidade de expor estas aplicações para a internet ou uso de VPN e deve suportar os mesmos métodos e protocolos do item anterior.

XVIII - A solução dever ser baseada em algoritmos de aprendizado de máquina (Machine Learning) não supervisionados, ou seja, os modelos estatísticos com os casos de uso já prontos e calibrados.

XIX - A solução deve medir o risco da autenticação verificando o comportamento histórico da identidade através do conjunto dos seguintes atributos:

a) Geolocalização: medindo o risco da autenticação verificando sua localização geográfica do acesso atual em comparação com o seu comportamento usual.

b) Dia da Semana: medindo o risco da autenticação verificando o dia da semana do acesso atual em comparação com seu comportamento usual.

c) Horário do Acesso: mede o risco da autenticação verificando o horário do acesso atual em comparação com seu comportamento usual.

d) Sistema Operacional: mede o risco da autenticação verificando o Sistema Operacional do acesso atual em comparação com seu comportamento usual

e) Falhas de login consecutivas, mede o risco da autenticação verificando as falhas de login consecutivas do acesso atual em comparação com seu comportamento usual

f) Deve prover a personalização das faixas de pontuação (0 a 100) para os administradores da solução para, no mínimo, as categorias:

- A) Sem risco
- B) Risco Baixo
- C) Risco Médio
- D) Risco Alto

XX - O risco calculado durante a autenticação pelo motor de análise do comportamento dos usuários deve ser compartilhado com funções de Múltiplo Fator de autenticação e Single Sign-On que realizam o login para os casos

de uso citados neste documento e utilizar como contexto para:

a) Requisitar múltiplos fatores de autenticação de forma dinâmica.

b) Permitir o login sem o uso de múltiplos fatores.

c) Negar a autenticação.

XXI - Deve prover para os administradores da solução a capacidade de explorar os dados históricos através de dashboards, filtros e gráficos configuráveis sendo possível verificar os alertas e os fatores que os influenciaram, além da exploração dos eventos capturados e seus atributos.

XXII - Deve prover gráficos de linha do tempo, donuts, mapas com geolocalização dos eventos, gráfico de barras, tabelas analíticas, e mapas de relacionamento, sendo suas dimensões e categorias personalizáveis

XXIII - Deve ser capaz de exportar os dados dos alertas, riscos calculados, eventos para, no mínimo, CSV, adicionalmente gravar as visualizações na solução para consultas posteriores.

XXIV - Deve possuir integração com fontes de inteligência cibernética de terceiros reconhecidas no mercado.

XXV - Deve possuir interface para envio de alertas de forma automatizada, suportando, no mínimo:

a) E-mail com conteúdo do alerta.

b) Webhooks (ex: envio de mensagem para um canal do Microsoft Teams ou Slack.

XXVI - Possuir dashboards pré-configurados com informações e gráficos com as seguintes características:

a) Utilização do modelo de Análise do Comportamento dos Usuários.

b) Comportamento dos usuários na utilização das aplicações.

c) Visão sobre a segurança das aplicações.

d) Mapa com a geolocalização das autenticações.

e) Visão sobre o comportamento dos Endpoints (Mobile e Computadores).

f) Visão sobre o comportamento das Identidades.

XXVII - A solução deve permitir a configuração de dashboards personalizados.

XXVIII - Deve permitir o compartilhamento dos dashboards com outros usuários.

XXIX - A solução deve permitir que as aplicações acessadas através do portal Single Sign-on sejam monitoradas e indexadas em uma linha do tempo, registrando a navegação do usuário na página web.

XXX - Deve registrar cliques de janela e textos utilizados durante a navegação do usuário final na aplicação monitorada.

XXXI - Deve permitir ao administrador, acessos a screenshots da navegação do usuário final na página web da aplicação, que identificam visualmente o campo modificado em destaque e o momento exato da ação durante a navegação.

XXXII - Deve permitir ao administrador pesquisar por meio da seleção de aplicações gerenciadas no portal e campos indexados, como textos e campos acessados durante a navegação.

XXXIII - Deve permitir o isolamento da sessão do browser para aplicações web monitoradas, não permitindo a função copiar e colar e qualquer tipo de download da sessão isolada, dessa forma evitando o vazamento de informações desta sessão web protegida.

XXXIV - Deve permitir gravação da sessões em nuvem, a fim de não onerar espaço de armazenamento on premisses do órgão contratante.

XXXV - Deve permitir iniciar gravação, monitoramento contínuo e isolamento de sessão web por aplicação e perfil de acesso.

XXXVI - Deve alertar o usuário final de maneira visual, antes de iniciar o processo de monitoramento e gravação da sessão.

Rio de Janeiro, 27 de abril de 2025

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 28/04/2025, às 17:19, 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 28/04/2025, às 17:27, 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 **Monique Goncalves Paz**, **Diretora**, em 28/04/2025, às 18:01, 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 **Rosana Alves de Andrade**, **Analista de Sistemas**, em 28/04/2025, às 18:22, 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 **98839100** e o código CRC **3BACC8BA**.

Referência: Processo nº SEI-430002/001509/2024 SEI nº 98839100

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

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 ESTUDO TÉCNICO PRELIMINAR

MAPA DE RISCOS

1. OBJETO

1.1. A análise dos riscos pretende identificar, avaliar e adotar respostas aos eventos de riscos do modelo de contratação proposto, de forma a assegurar o alcance do objetivo da contratação, por meio da identificação antecipada dos possíveis eventos que poderiam ameaçar o processo licitatório, a execução contratual, o cumprimento das obrigações contratuais, etc.

1.2. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar do qual é parte integrante e indissociável.

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

2.1. 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.

2.2. 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

2.3. 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

2.4. 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.

2.5. 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.

2.6. 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	Não Indicação de servidores pelas áreas envolvidas no processo de aquisição para compor a Equipe de Planejamento da Contratação para elaborar a documentação necessária	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R2	Levantamento inadequado dos itens	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R3	Edital e Termo de Referência incompletos ou inconsistentes	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R4	Insuficiência de recursos orçamentários para contratação dos serviços	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R5	Não autorização de despesa para a contratação	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R6	Erro na pesquisa das quantidades necessárias para a licitação	infraestrutura	média (10)	alto (15)	150	Aceitação Ativa / Mitigar
R7	Demora na conclusão do processo licitatório, ocasionando atrasos na homologação e consequente contratação	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R8	Recusa do licitante vencedor em assinar o contrato	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R9	Atraso na entrega dos equipamentos (itens do objeto contratado)	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R10	Quantitativo de pessoal ou capacitação insuficiente dos agentes de fiscalização e gestão do contrato	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R11	Contratada fornecer bem fora dos padrões pretendidos	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R12	Falência, insolvência, quebra contratual pela contratada	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R13	Falta de disponibilidade financeira para pagamento de despesa no prazo	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R14	Não aplicação de sanções à contratada pela Administração	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R15	Ausência de interessados na licitação como um todo ou em algum/alguns lotes do certame	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R16	Exclusão da DSI quanto ao estabelecimento das políticas e regras para a configuração da solução.	infraestrutura	média (10)	alto (15)	150	Aceitação Ativa / Mitigar

3. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

Em atendimento ao art. 38, II e III da IN SGD/ME nº 01/2019 (a título de boas práticas).

RISCO 1			
Não Indicação de servidores pelas áreas envolvidas no processo de aquisição para compor a Equipe de Planejamento da Contratação para elaborar a documentação necessária.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta

Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato	
Id	**Dano**	
1.1.	Atraso na contratação;	
	Contratação em desacordo com a necessidade da Administração.	
Id	**Ação Preventiva**	**Responsável**
1.1.1.	Designar pessoal das áreas envolvidas na contratação para a composição da equipe de planejamento da contratação.	Diretores das Áreas Envolvidas
Id	**Ação de Contingência**	**Responsável**
1.1.2.	Refazer a documentação de acordo com a necessidade da Administração.	Equipe de Planejamento da Contratação

RISCO 2			
Levantamento inadequado dos itens.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
2.1.	Não alcançar todas as necessidades e resultados pretendidos.		
Id	**Ação Preventiva**		**Responsável**
2.1.1.	Verificar a eventual adequação das especificações por ocasião da elaboração do Termo de Referência.		Responsáveis pelo Termo de Referência
Id	**Ação de Contingência**		**Responsável**
2.1.2.	Verificar a documentação já utilizada por outros Órgãos recentemente.		Responsáveis pelo Termo de Referência

RISCO 3			
Edital e Termo de Referência incompletos ou inconsistentes.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
3.1.	Licitação fracassada;		

	Contratação em desacordo com a necessidade da Administração; Prejuízo ao erário

Id	Ação Preventiva	Responsável
3.1.1.	Revisar cuidadosamente o Edital e o Termo de Referência, de modo a verificar suas adequações.	Equipe de Planejamento da Contratação, GEA
Id	**Ação de Contingência**	**Responsável**
3.1.2.	Revogar ou anular o processo de licitação.	VPT / VPA

RISCO 4			
Insuficiência de recursos orçamentários para contratação dos serviços.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		

Id	Dano	
4.1.	Inviabilidade de execução contratual.	
Id	**Ação Preventiva**	**Responsável**
4.1.1.	Prever recursos necessários no orçamento anual.	DOF
Id	**Ação de Contingência**	**Responsável**
4.1.2.	Readequar a contratação à capacidade orçamentária disponível.	Equipe de Planejamento da Contratação

RISCO 5			
Não autorização de despesa para a contratação			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		

Id	Dano	
5.1.	Inviabilidade de execução contratual.	
Id	**Ação Preventiva**	**Responsável**
5.1.1.	Prever recursos necessários no orçamento anual.	DOF
Id	**Ação de Contingência**	**Responsável**

5.1.2.	Readequar a contratação à capacidade orçamentária disponível.	Equipe de Planejamento da Contratação

RISCO 6		
Erro na pesquisa das quantidades necessárias para a licitação.		
Probabilidade:	( ) Baixa (x) Média	( ) Alta
Impacto:	( ) Baixa ( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato	
Id	**Dano**	
6.1	Impedimento da contratação por erro nos quantitativos.	
Id	**Ação Preventiva**	**Responsável**
6.1.1	Melhorar a pesquisa junto aos Órgãos e Secretarias do Estado do Rio de Janeiro.	GEA
Id	**Ação de Contingência**	**Responsável**
6.1.2	Revogar ou anular o processo de licitação.	VPA

RISCO 7			
Demora na conclusão do processo licitatório, ocasionando atrasos na homologação e consequente contratação.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória (x) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
7.1.	Atraso na contratação.		
Id	**Ação Preventiva**		**Responsável**
7.1.1.	Designar pessoal capacitado e em quantidade suficiente para a condução do processo licitatório.		Presidente / VPA
Id	**Ação de Contingência**		**Responsável**
7.1.2.	Designar pessoal adicional para a condução do processo licitatório.		Presidente / VPA

RISCO 8

Recusa do licitante vencedor em assinar o contrato			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
8.1.	Impossibilidade de iniciar a execução dos serviços.		
Id	**Ação Preventiva**		**Responsável**
8.1.1.	Verificar situações que possam ensejar a inexequibilidade contratual.		AJU
Id	**Ação de Contingência**		**Responsável**
8.1.2.	Refazer os procedimentos de contratação.		GGC / AJU

RISCO 9			
Atraso na entrega dos serviços			
Probabilidade:	(x) Baixa		( ) Média ( ) Alta
Impacto:	( ) Baixa		( ) Média (x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
9.1.	Ativos (sites e aplicações) desprotegidos com maior risco de ciberataques aos sistemas do Governo do Estado.		
Id	**Ação Preventiva**		**Responsável**
9.1.1.	Comunicar ao fornecedor, três dias antes do prazo, e exigir celeridade na entrega, visto que o processo licitatório foi concluído.		Gestor do Contrato
Id	**Ação de Contingência**		**Responsável**
9.1.2.	Decidir sobre a realização da rescisão contratual.		VPT / VPA

RISCO 10			
Quantitativo de pessoal ou capacitação insuficiente dos agentes de fiscalização e gestão do contrato			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		

10.1.	Falha no acompanhamento da gestão contratual	
Id	**Ação Preventiva**	**Responsável**
10.1.1.	Designar pessoal qualificado no objeto e em quantidade suficiente	PRE
	Realizar capacitação de equipe	VPA
	Realizar reuniões periódicas para atualização dos procedimentos de fiscalização contratual e compartilhamento de informações	Comissão de Fiscalização
Id	**Ação de Contingência**	**Responsável**
10.1.2.	Atribuição das atividades de gestão e fiscalização do contrato a outros servidores que já estejam capacitados	Equipe de planejamento da contratação

RISCO 11			
Contratada fornecer serviços fora dos padrões pretendidos.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
11.1.	Aquisição de uma solução de WAAP abaixo das exigências técnicas definidas, acarretando danos ao erário		
Id	**Ação Preventiva**		**Responsável**
11.1.1.	Acompanhar e cobrar da contratada o fornecimento dos equipamentos contratados dentro dos padrões pretendidos. Não realizar o recebimento dos bens fora dos padrões pretendidos		Fiscais do Contrato
	Não realizar o recebimento do objeto fora dos padrões pretendidos		
Id	**Ação de Contingência**		**Responsável**
11.1.2.	Notificar a contratada pelo descumprimento de obrigação contratual;		Gestor do Contrato
	Exigir a entrega de equipamentos em conformidade com o que foi disciplinado no Termo de Referência.		

RISCO 12			
Falência, insolvência, quebra contratual pela contratada.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		

12.1.	Interrupção imediata do contrato	
Id	**Ação Preventiva**	**Responsável**
12.1.1.	Acompanhar as condições de habilitação da contratada, em especial quanto à qualificação econômico-financeira.	GGC
Id	**Ação de Contingência**	**Responsável**
12.1.2.	Reavaliar as empresas existentes no mercado para compra emergencial enquanto se elabora novo instrumento licitatório	GGC / DAF / GEA / DSI

RISCO 13			
Falta de disponibilidade financeira para pagamento de despesa no prazo			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
13.1.	Cometimento de ato ilegal; Prejuízo ao erário no caso de exigência por parte da contratada de pagamento em valor corrigido		
Id	**Ação Preventiva**		**Responsável**
13.1.1.	Obedecer à ordem de pagamentos conforme entrada no setor financeiro.		DOF / GOF
Id	**Ação de Contingência**		**Responsável**
13.1.2.	Solicitar repasse de recurso ao Tesouro para realizar pagamento no prazo.		DOF / GOF

RISCO 14			
Não aplicação de sanções à contratada pela Administração			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
14.1.	Prejuízo ao erário; Manutenção de empresa inadequada no mercado.		
Id	**Ação Preventiva**		**Responsável**
14.1.1.	Notificar a contratada por falhas na execução contratual.		GGC / Gestor do Contrato

Id	Ação de Contingência	Responsável
14.1.2.	Instaurar processo sancionador para eventual aplicação de sanção.	GGC / AJU

RISCO 15			
Ausência de interessados na licitação como um todo ou em algum/alguns lotes do certame			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória (x) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
14.1.	Licitação deserta ou fracassada Falta do fornecimento pretendido		
Id	**Ação Preventiva**		**Responsável**
14.1.1.	Realização de pesquisa de preços ampla		Equipe de planejamento
Id	**Ação de Contingência**		**Responsável**
14.1.2.	Repetição do certame ou contratação direta, na forma do artigo 75, III, da Lei nº 14.133/2021, se o certame, justificadamente, não puder ser repetido sem prejuízo para a Administração		VPA

RISCO 16			
Exclusão da DSI quanto ao estabelecimento das políticas e regras para a configuração da solução.			
Probabilidade:	( ) Baixa	(x) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
16.1.	Prejuízo em políticas e regras que possam abrir vulnerabilidades no ambiente de rede a ser protegid		
Id	**Ação Preventiva**		**Responsável**
16.1.1.	Exigir que os setores competentes participem da criação das políticas, de modo que sejam construídas conjuntamente entre as áreas de infraestrutura e segurança.		VPT
Id	**Ação de Contingência**		**Responsável**
16.1.2.	Refazer e implementar as políticas da solução		DSI e DIT

Rio de Janeiro, 17 de fevereiro de 2025

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 28/04/2025, às 17:19, 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 28/04/2025, às 17:27, 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 **Monique Goncalves Paz**, **Diretora**, em 28/04/2025, às 18:01, 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 **Rosana Alves de Andrade**, **Analista de Sistemas**, em 28/04/2025, às 18:24, 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 **98839125** e o código CRC **A4938129**.

Referência: Processo nº SEI-430002/001509/2024 SEI nº 98839125

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

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 ESTUDO TÉCNICO PRELIMINAR

1. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar do qual é parte integrante e indissociável.
2. Para fins de quantificação de cada um dos itens componentes do objeto proposto, os Órgãos interessados em participar deste Sistema de Registro de Preços devem observar as considerações constantes o quadro a seguir:

LOTE ÚNICO					
Item	**ID SIGA/RJ**	**Descrição**	**Métrica**	**Justificativa**	**Forma de quantificação**
1	189256	Subscrição de Licença para Proteção Local e Elevação de Privilégio em servidores, com suporte técnico, por de 12 (doze) meses	unidade	Este módulo da solução permitirá a proteção dos servidores (item 1) e estações de trabalho (item 2) no que diz respeito a contas privilegiadas, garantindo acesso controlado a essas contas apenas por usuários autorizados.	por servidor
2	189257	Subscrição de Licença para Proteção Local e Elevação de Privilégio em desktops, com suporte técnico, por 12 (doze) meses	unidade		por desktop
3	189258	Subscrição de Solução de Autenticação Multifator Adaptativa, com suporte técnico, por 12 (doze) meses	unidade	Este módulo da solução permitirá a implementação de múltiplos fatores de autenticação baseado em risco para os usuários.	por pessoa
4	189259	Subscrição de Solução de Logon Único Adaptativo para Identidades dos Colaboradores, com suporte técnico, por 12 (doze) meses	unidade	Este módulo agrega na solução o método de autenticação Single Sign On (SSO).	por pessoa
5	189263	Treinamento operacional para solução de Proteção Local e Elevação de Privilégio em servidores	turma	Serviço opcional de treinamento em cada um dos módulos da solução. Recomendável, dada a complexidade da ferramenta.	Por quantidade de alunos a serem treinados em cada módulo. Até 6 alunos por turma. O órgão deve aderir somente aos treinamentos correspondentes a itens de subscrição que ele mesmo contratou (dentre os itens 1 a 4).
6	189264	Treinamento operacional para solução de Proteção Local e Elevação de Privilégio em desktops	turma		
7	189265	Treinamento operacional para solução de Autenticação Multifator Adaptativa	turma		
8	189266	Treinamento operacional para solução de Logon Único Adaptativo para Identidades dos Colaboradores	turma		

Rio de Janeiro, 27 de abril de 2025

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 28/04/2025, às 17:19, 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 28/04/2025, às 17:27, 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 **Monique Goncalves Paz**, **Diretora**, em 28/04/2025, às 18:01, 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 **Rosana Alves de Andrade**, **Analista de Sistemas**, em 28/04/2025, às 18:24, 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 **98839138** e o código CRC **D0DA9521**.

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