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

SOLUÇÃO DE GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1.1. A presente contratação justifica-se tendo em vista o atendimento das demandas encaminhadas por órgãos da Administração na forma dos Ofícios SECC/SUBGE nº 20/2024 (82469542), DER/GABPRES nº 668 (82470543) e SEIOP/GABSEC nº 844 (82471158), os quais manifestaram interesse por uma solução de mapeamento, classificação, anonimização e pseudonimização de dados em repouso e em trânsito, incluindo serviços de instalação e configuração da solução e serviços especializados para suportar e implantar a solução.

1.2. O Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ, através da Diretoria de Segurança da Informação, na forma do Documento de Oficialização de Demanda instruído no processo SEI-430002/001510/2024, desenvolveu o presente Estudo Técnico Preliminar – ETP, de forma a reunir o conjunto de informações indicativas e as condições preliminares voltadas para uma SOLUÇÃO DE GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS, de forma a propiciar o aproveitamento por outros órgãos da Administração Pública, com vistas à mitigação e combate de ameaças de segurança cibernética que afetam a rede governo.

1.3. Este ETP constitui etapa do Planejamento da Contratação, tendo por base a Lei Federal nº 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.

1.4. A contratação de SOLUÇÃO DE GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS deverá abranger a plataforma de gerenciamento de chaves criptográficas, controle de acesso, visibilidade e rastreabilidade de utilização de dados em servidores de arquivos, banco de dados, infraestrutura em nuvem (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS), incluindo serviço de instalação e configuração da solução, integrações necessárias com soluções de terceiros e serviços especializados.

1.5. A necessidade ou problema a ser resolvido com a solução de gerenciamento de chaves criptográficas está relacionada à proteção de dados pessoais de modo geral e, portanto, ao cumprimento de regulamentações de privacidade, como a Lei Federal nº 13.709/2018, ou Lei Geral de Proteção de Dados (LGPD).

1.6. Em termos simples, dados anonimizados são aqueles relativos a determinado titular que não possa ser identificado, levando-se em consideração a utilização de ferramentas técnicas razoáveis e disponíveis por ocasião do tratamento. Por sua vez, dados pseudonimizados seriam aqueles que possuem a possibilidade de reversão do seu processo de anonimização, ou seja, seria uma técnica de mascaramento dos dados, que pode ter suas informações recuperadas a qualquer momento pelo operador.

1.7. A anonimização de dados pessoais é uma demanda tecnológica trazida pela LGPD, que transfere para as empresas a responsabilidade pela segurança dos dados sob sua guarda. A necessidade de implementar uma solução de anonimização de dados e gerenciamento de chaves de criptografia, portanto, surge da crescente demanda por segurança da informação e conformidade com as regulamentações de proteção de dados.

1.8. A anonimização de dados é um processo crítico de segurança cibernética que permite a utilização de informações para fins analíticos, de pesquisa ou compartilhamento, sem comprometer a identidade dos titulares dos dados. O gerenciamento de chaves de criptografia é essencial para garantir que os dados sensíveis sejam protegidos contra acessos não autorizados, vazamentos ou violações.

1.9. A implementação de SOLUÇÃO DE GERENCIAMENTO DE CHAVES CRIPTOGRÁFICAS constitui papel fundamental na manutenção e disponibilidade adequada aos serviços e à continuidade das operações institucionais e corporativas dos órgãos do ERJ, apoiando as divisões de infraestrutura e de segurança da informação, de forma a manter a integridade, segurança e disponibilidade dos dados sob sua custódia.

1.10. Tendo em vista o atendimento à três órgãos demandantes, bem como observadas as disposições do art. 3º, inciso III do Decreto Estadual nº 48.843/2023, se faz necessária a utilização de Sistema de Registro de Preços em eventual licitação que venha a ser procedida para fins de aplicação da solução tecnológica aqui tratada.

- Decreto Estadual nº 48.843/2023
- art. 3º O SRP deverá ser adotado, preferencialmente, nas seguintes hipóteses:
- (...)
- III - quando for conveniente para atendimento a mais de um órgão ou entidade, bem como aos programas de governo (...)

1.11. A título de informação, o PRODERJ já manteve Ata de Registro de Preços nº 01/2023 com vigência expirada em 14.02.2024, conduzida no âmbito do SEI-150016/000789/2021, cujo objeto tratou de solução de "Anonimização e Gerenciamento de Chaves Criptográficas".

1.12. Justificativa

1.12.1. Com o advento da Lei Estadual nº 9.128/2020, que dispõe sobre a transformação digital dos serviços públicos, bem como do Decreto Estadual nº 48.671/2023, que institui o Portal Único RJ DIGITAL e dispõe sobre as regras de unificação dos canais digitais do Governo do Estado do Rio de Janeiro no âmbito da Administração Pública Direta, Autárquica e Fundacional, a Secretaria Estadual de Transformação Digital (SETD) vem empenhando esforços na busca da plena digitalização dos serviços públicos estaduais oferecidos aos cidadãos fluminenses, com a extinção gradual do "atendimento de balcão".

1.12.2. Tal cenário torna necessária a adoção de soluções de proteção de aplicações, de modo a estabelecer um modelo de proteção para informações em que os dados sejam devidamente criptografados no sistema de arquivos. Assim, além de impedir a extração não autorizada, mesmo em caso de vazamento acidental dos dados, deve-se garantir que os dados não possam ser acessados fora do ambiente gerenciado pela plataforma de segurança, uma vez que neste caso hipotético o destino não possuiria a chave criptográfica necessária para a decodificação, impedindo o acesso às informações sensíveis.

1.12.3. 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.

1.12.4. Diante o exposto, se torna essencial que a Autarquia promova a garantia dos três pilares da segurança da informação a nível Estadual, preconizada na ISO/IEC 27.000, quais sejam, confidencialidade, integridade e disponibilidade das informações. O comprometimento de apenas um desses pilares, mesmo que momentâneo, em decorrência de tentativas de sequestro de dados ou ataques cibernéticos de qualquer escala, resultam em danos incomensuráveis aos usuários dos serviços prestados através de qualquer sistema. O principal prejudicado é o cidadão, que têm atendidas suas necessidades básicas através de tais serviços.

1.12.5. Nesse contexto, também cabe 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.

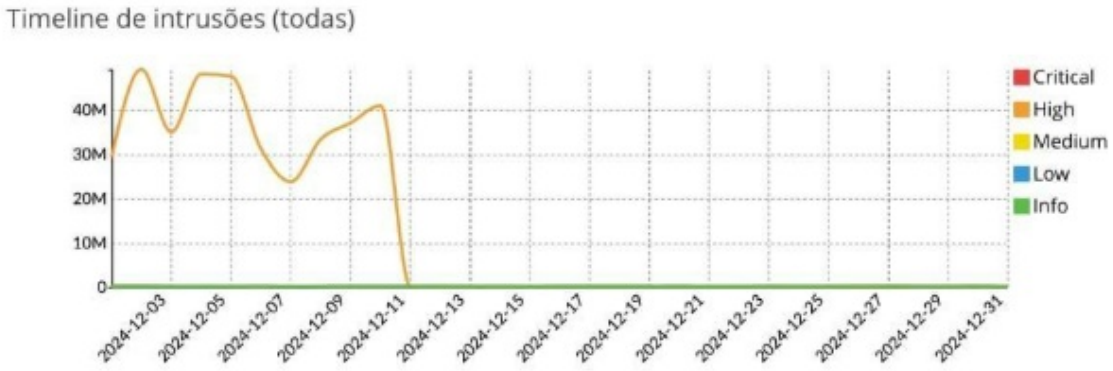
1.12.6. Para o sucesso no desempenho dessas atribuições, é fundamental que o PRODERJ proporcione a todo o Estado do Rio de Janeiro os níveis de segurança compatíveis com o papel que desempenha.

1.12.7. Portanto, para assegurar a total proteção e a garantia do sigilo dessas informações, no caso de possíveis invasões, sequestros de dados ou de informações de extrema relevância, o PRODERJ vem buscando no mercado mecanismos de proteção a aplicações web, de forma a melhorar os níveis de confidencialidade, integridade e disponibilidade dessas aplicações, de forma automatizada e segura.

1.12.8. A tarefa de manter a área de TIC sempre alinhada às estratégias do PRODERJ constitui-se um desafio permanente. Busca-se garantir, em todas as questões relacionadas à infraestrutura de TI do Estado do Rio

de Janeiro, que o foco se mantenha na estratégia e nas necessidades finalísticas desta Autarquia. Além disso, existe também a tarefa e obrigação de manter o ambiente tecnológico do Estado em alta disponibilidade e de preservar a qualidade dos serviços por ele providos sempre alinhados às estratégias do PRODERJ.

1.12.9. 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 de dezembro/2024, com as estatísticas de tentativas de ataques ocorridos no peíodo:



Ameaças por severidade

High	376,604,637
Critical	1,448,132
Info	754,552
Low	609,003
Medium	102,209

1.12.10. As aplicações da web estão em constante evolução e se tornando mais complexas, com novos desafios de segurança de aplicações para as organizações. Com maior frequência, as aplicações da web e os micros serviços modernos dependem de API's para quase todas as interações, o que expande a superfície de ataque com novos possíveis pontos de entrada para os hackers. Conforme a superfície de ataque às aplicações aumenta, os cybers criminosos respondem com ataques multi vetoriais cada vez mais sofisticados. Muitas vezes, fazendo uso de bots automatizados, botnets e scanners de vulnerabilidades, os invasores conseguem invadir ambientes de TIC com sucesso e assumir contas de usuários para roubar dados, transferir fundos para contas fraudulentas, interromper operações de negócios e iniciar ataques cibernéticos devastadores. Desse modo, ainda que ocorram esses tipos de ataques, inevitavelmente, é dever do PRODERJ promover a preservação dos dados "sequestrados" para que não haja prejuízo ao poder público e aos usuários dos sistemas.

1.12.11. A ferramenta contribuirá para o atendimento da Lei Federal nº 13.709/2018 (LGPD), que intensifica a obrigatoriedade de proteção e privacidade dos dados dos titulares, no nosso caso, os cidadãos, reforçando a necessidade do PRODERJ, Órgão de Tecnologia do Estado, contratar e fornecer aos demais Órgãos da Administração Pública 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.

1.12.12. O presente estudo se embasa, portanto, 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.

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

ATUAL

2.1. **Contratações anteriores**

2.1.1. O PRODERJ implantou uma camada de proteção de anonimização de dados por meio de licitação em Sistema de Registro de Preços conduzida no processo SEI-150016/000789/2021, do qual resultou a Ata de Registro de Preços nº 01/2023, cuja vigência expirou em 14.02.2024.

2.1.2. Mediante os Contratos de compra nº 026/2023 (SEI-430002/000503/2023) e nº 07/2024 (SEI-430002/000181/2024) o PRODERJ adquiriu, na modalidade perpétua, os softwares abaixo listados com suas respectivas quantidades na TABELA 1 abaixo:

TABELA 1			
Item	**Descrição**	**Métrica**	**Quantidade**
1	CONSOLE DE GERENCIAMENTO centralizado em alta disponibilidade, incluindo licenciamento permanente, instalação e configuração	UN	2
3	AGENTES DE PROTEÇÃO DADOS PARA BANCO DE DADOS, incluindo licenciamento permanente, instalação e configuração	UN	10
5	AGENTES PARA COMPARTILHAMENTO SEGURO DE BASE DE DADOS, incluindo licenciamento permanente, instalação e configuração	UN	1
7	AGENTES DE PROTEÇÃO DE DADOS PARA SERVIDORES DE ARQUIVO (FILE SERVER), incluindo licenciamento permanente, instalação e configuração	UN	7
9	AGENTES DE PROTEÇÃO DE DADOS PARA CONTÊINERES, incluindo licenciamento permanente, instalação e configuração	UN	15
11	AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO, incluindo licenciamento permanente, instalação e configuração	UN	21
14	AGENTES PARA GESTAO DE CHAVES LOCAL, incluindo licenciamento permanente, instalação e configuração	UN	2

2.1.3. Através dos Contratos de serviço nº 025/2023 (SEI-430002/000503/2023) e nº 08/2024 (SEI-430002/000181/2024), o PRODERJ adquiriu, na forma da TABELA 2 abaixo, os respectivos suportes técnicos em categoria avançada para os softwares informados no subtópico anterior, bem como a subscrição do software de agentes para descoberta e classificação de dados (anuidade de licença):

TABELA 2			
Item	**Descrição**	**Métrica**	**Quantidade**
2	Serviço de manutenção, atualização de versão e garantia para CONSOLE DE GERENCIAMENTO	UN	2
4	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DADOS PARA BANCO DE DADO	UN	10
6	Serviço de manutenção, atualização de versão e garantia para AGENTES PARA COMPARTILHAMENTO SEGURO DE BASE DE DADOS	UN	1
8	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DE DADOS PARA SERVIDORES DE ARQUIVO (FILE SERVER)	UN	7
10	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DE DADOS PARA CONTÊINERES	UN	15
12	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO	UN	21
13	Subscrição de agentes para gestão de chaves na nuvem, incluindo instalação e configuração	UN	2
15	Serviço de manutenção, atualização de versão e garantia para AGENTES PARA GESTAO DE CHAVES LOCAL	UN	2
16	Subscrição de agentes para descoberta e classificação de dados, incluindo instalação e configuração. Termo de Licenciamento por 12 (doze) meses (Franquia 50 TB)	UN	1
17	Serviço de treinamento para solução de gerenciamento de chaves criptográficas	Aluno	6
18	Serviço de operação assistida para solução de gerenciamento de chaves criptográficas	UST	2.000

2.1.4. A plataforma atualmente contratada pelo PRODERJ, constituída dos itens informados nas TABELAS 1 e 2 acima, atende a servidores do Banco de Dados.

2.1.5. A mesma plataforma foi contratada por outros órgãos da Administração, a exemplo do DETRAN (Contrato nº 037/2023 - SEI- 150112/000123/2021), da Secretaria de Estado de Transportes (Contrato nº 18/2023 - SEI-100001/002569/2023), do Rio Previdência (Contrato nº 078/2023 - SEI-040161/011328/2023), da AGETRANSP (Contrato nº 16/2023 - SEI-100007/000222/2023), da Secretaria de

Estado de Saúde (Contrato nº 044/2023 - SEI-080001/011789/2023), da CEDAE (Contrato nº 023/2024 - SEI-150001/030934/2024 e da Secretaria Estadual de Polícia Civil (Contrato nº 008/2024 - SEI-360016/000066/2024.

2.2. **Contratações correlatas ou interdependentes**

2.2.1. Não há contratações interdependentes ou correlatas à presente, uma vez que o objeto em tela não compõe, no todo ou em parte, objetos ou soluções de outras contratações.

2.2.2. Observado pelo exposto no subtópico anterior, que muito embora o PRODERJ tenha celebrado os contratos nºs 25 e 26/2023 e nºs 07 e 08/2024, cujos objetos são semelhantes ao descrito no presente ETP, que não há correlação ou interdependência entre as contratações, uma vez que o Registro de Preços futuro tem por finalidade o atendimento dos três órgãos demandantes já citados no subtópico 1.3.

2.2.3. Ademais, os três órgãos demandantes não realizaram a contratação desta solução no âmbito da Ata de Registro de Preços já expirada, de modo que não existe correlação ou interdependência também para estes casos.

3. INSTRUMENTOS DE PLANEJAMENTO

3.1. Demonstração da previsão da contratação no Plano de Contratações Anual - PCA do PRODERJ: Não há expectativa de contratação da presente solução pelo PRODERJ.

3.2. Os órgãos participantes de Sistema de Registro de Preços deverão prever o objeto tratado neste estudo em seus Planos Anuais de Contratação, devidamente catalogados perante o Portal Nacional de Compras Públicas (PNCP) do Governo Federal.

4. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

A presente contratação orienta-se pelos seguintes requisitos:

4.1. **Requisitos de Negócio**

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

I - Contratação de plataforma de anonimização e gerenciamento de chaves criptográficas, controle de acesso, visibilidade e rastreabilidade de utilização de dados em servidores de arquivos, banco de dados, infraestrutura em nuvem (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS), incluindo serviço de instalação, configuração da solução, integrações necessárias com soluções de terceiros e serviços especializados, conforme Anexo I (Especificações Técnicas do Objeto) deste documento;

II - Treinamentos operacionais das soluções contratadas, voltados para os técnicos da CONTRATANTE;

III - A solução tecnológica utilizada na prestação dos serviços deverá estar disponível para acesso da CONTRATANTE, ininterruptamente, 24h por dia, 7 dias por semana, durante todo o período contratual;

IV - A solução deverá apresentar as seguintes características gerais:

a) Agentes e módulos: a solução deverá prover agentes de proteção de dados para banco de dados, agente de proteção de dados para containers, servidores de arquivo (file server), aplicações web, agentes para compartilhamento seguro de bases de dados, agentes para gestão de chave local, módulo de identificação e classificação de dados;

b) Gerenciamento integrado e centralizado dos agentes de criptografia: a solução deverá prover uma console única permita o gerenciamento centralizado de todos os agentes de criptografia, suas chaves criptográficas, políticas de configuração, publicação e controle de acesso dos dados a serem protegidos;

c) Controle de acesso: deve prover controle de acesso de usuários, incluindo usuários privilegiados, registro detalhado de auditoria de acesso, visando atender aos requisitos de conformidade, e práticas recomendadas. As políticas de controle de acesso deverão permitir ser aplicadas mesmo aos usuários privilegiados do sistema e estes não deverão possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio;

d) Proteção e controle de acesso a bancos de dados: a solução deve oferecer recursos para proteger e controlar o acesso a bancos de dados, arquivos e contêineres. Além de poder

proteger ativos que residem em nuvem, servidores virtuais, big data e servidores físicos. A solução deverá prover ainda uma console de gerenciamento composta por um conjunto integrado de produtos baseados em uma infraestrutura comum e extensível, com gerenciamento centralizado de políticas e de chaves;

e) Recursos de criptografia: além de criptografar o banco de dados, os agentes deverão ser capazes de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações estruturadas e não estruturadas. Os agentes deverão registrar e rastrear o acesso dos usuários aos arquivos e ser capaz de bloquear ou restringir este acesso.

4.1.2. Com relação ao subtópico 4.1.1, inciso I, entende-se como “configuração da solução” o conjunto de intervenções minimamente necessárias a possibilitar o start da aplicação, após a fase de instalação, não se tratando de demais configurações decorrentes ou inerentes às atividades de suporte técnico ou de operação assistida (nível usuário), as quais são pertinentes ao "Catálogo de Serviços" previsto neste documento.

4.2. **Requisitos de Capacitação**

4.2.1. A capacitação compreende os serviços de treinamentos na aplicação.

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

4.2.3. Deverá ser entregue para a CONTRATANTE, no momento da reunião kick off prevista neste documento, o programa e a proposta com o conteúdo do treinamento, para aprovação prévia da Fiscalização.

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.

4.2.5. A troca de instrutor também poderá ser solicitada caso, comprovadamente, este não esteja ministrando o treinamento de forma compatível com o conteúdo programático aprovado pela Fiscalização (item 4.2.3), ou por excesso de faltas não justificadas. Nesses casos, poderá também ser solicitada a repetição total ou parcial do treinamento, quando necessário.

4.2.6. O treinamento deverá ser ministrado por instrutor capacitado na solução, com certificação na ferramenta expedida pelo fabricante (mediante apresentação de cópia), de forma a garantir que o treinamento seja conduzido de modo adequado e pertinente ao que a solução contratada oferecerá, em todas as suas funcionalidades.

4.2.7. Deverão ser fornecidos pela CONTRATADA os certificados de capacitação (certificado de conclusão do curso) para os participantes do treinamento, atestando que os mesmos estão aptos à utilização da ferramenta. O treinamento demandado por aluno (vaga), e as turmas deverão ser limitadas a 10 (dez) alunos, conforme o item 10.4.

4.2.8. A carga horária do treinamento deverá ser de no mínimo 40h, sem qualquer ônus adicional para a CONTRATANTE.

4.2.8.1. O treinamento deverá ter início no prazo máximo de até 20 dias úteis, contados a partir do início da instalação da solução, quando o CONTRATANTE não especificar outros prazos.

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

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

4.2.9. **Forma de realização**

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

4.2.10. **Materiais didáticos e acessórios**

4.2.10.1. 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.

4.2.10.2. O material didático será fornecido pela CONTRATADA no idioma português, abordando todos

os tópicos do curso.

4.2.11. **Conteúdo programático**

4.2.11.1. 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.

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

4.2.11.3. O treinamento deverá contemplar todos os recursos e configurações existentes na solução ofertada.

4.3. **Requisitos Legais**

4.3.1. Lei Federal nº 13.709/2018, Lei Geral de Proteção de Dados (LGPD);

4.3.2. Lei Federal nº 13.965/2014, Marco Civil da Internet;

4.3.3. Lei Federal nº 12.527/2011, Lei de Acesso à Informação (LAI);

4.3.4. Lei Estadual nº 9.128/2020, que dispõe sobre a transformação digital dos serviços públicos no âmbito do Governo do Estado do Rio de Janeiro;

4.3.5. Normas da Agência Nacional de Proteção de Dados (ANPD);

4.3.6. Decreto Estadual nº 48.671/2023, que institui o Portal Único RJ DIGITAL e dispõe sobre as regras de unificação dos canais digitais do Governo do Estado do Rio de Janeiro;

4.3.7. Decreto Estadual 48.997/2024, que dispõe sobre a reestruturação do Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC e estabelece as competências do PRODERJ enquanto órgão de Direção Geral do SETIC/RJ;

4.3.8. Instrução Normativa SLTI/MP nº 94/2022 (a título de boas práticas), que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC;

4.3.9. Nota técnica SGE TCE-RJ nº 06/2023, que orienta os jurisdicionados do TCE-RJ acerca da realização do planejamento para aquisição de bens e serviços de Tecnologia da Informação (TI) visando a atender ao princípio da economicidade;

4.3.10. ISO 27001:2022.

4.4. **Requisitos de Manutenção**

4.4.1. Todas as rotinas e insumos necessários para fins de manutenção com vistas ao pleno e adequado funcionamento das soluções ao longo da vigência contratual estarão a cargo da CONTRATADA, sem qualquer ônus para a CONTRATANTE, sendo o modo de prestação do serviço de Suporte Técnico previsto neste documento.

4.4.2. Caso se faça necessário eventual prestação de suporte nas dependências da CONTRATANTE, a CONTRATADA:

4.4.3. Deverá exigir dos seus empregados, o uso obrigatório de uniformes e crachás de identificação;

4.4.4. Não poderá se utilizar da presente situação para obter qualquer acesso não autorizado às informações de propriedade da CONTRATANTE;

4.4.5. Não poderá obter, capturar, copiar ou transferir qualquer tipo informação, física ou digital, de propriedade do CONTRATANTE, sem autorização.

4.5. **Requisitos Temporais**

4.5.1. Resguardados os cronogramas previstos no subtópico 25.2.1 deste documento, não há outros requisitos temporais a serem considerados.

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

4.6.1. Não se vislumbra, nesta análise, que o objeto acarretará impactos ambientais durante a prestação de serviços.

4.7. **Requisitos Tecnológicos**

4.7.1. **De arquitetura tecnológica**

4.7.1.1. Os requisitos tecnológicos de arquitetura das soluções encontram-se no Anexo I - Especificações Técnicas do Objeto.

4.7.1.2. O Catálogo de Serviços correspondentes à Operação Assistida encontra-se no subtópico 4.8.3.12 deste documento.

4.7.1.3. Durante a reunião de Kick-off prevista neste documento, a CONTRATADA deverá apresentar a arquitetura das soluções (Plano de Instalação) para a CONTRATANTE, que poderá aceitar ou propor nova arquitetura, para que então 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.

4.7.1.4. As seguintes atividades fazem parte do escopo das atividades de instalação e configuração inicial

a) Elaboração e entrega pela CONTRATADA do Plano de Instalação com os requisitos técnicos para a instalação e configuração da plataforma, tais como recursos computacionais, físicos, lógicos e de rede necessários, a serem disponibilizado pelo CONTRATANTE;

b) Instalação de todos os componentes da plataforma no ambiente disponibilizado, na versão recomendada pelo fabricante ou mais recente, por parte da CONTRATADA;

c) Aplicação do licenciamento, pela CONTRATADA, em todos os componentes da plataforma.

4.7.2. **Do projeto / Reunião Kick Off**

4.7.2.1. A CONTRATADA deve realizar nas dependências da CONTRATANTE, ou através de vídeo conferência (se viável), 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 inicial da solução.

4.7.2.2. Após a reunião de Kick-off, a CONTRATADA deverá produzir e entregar ao CONTRATANTE um Plano de Instalação contemplando o planejamento, escopo, cronograma, 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.

4.7.3. **Da implantação**

4.7.3.1. Compreende-se nesta etapa a instalação de equipamentos, sistemas, softwares e aplicativos da CONTRATANTE dos PRODUTOS, bem como a migração das configurações existentes na CONTRATANTE para os produtos fornecidos pela CONTRATADA, caso haja viabilidade, observadas as previsões acerca de requisitos materiais do subtópico 4.9.1 deste documento.

4.7.3.2. A etapa de instalação e configuração inicial deve acontecer de forma gradual e transparente, conforme o cronograma do CONTRATANTE.

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

4.7.3.4. As atividades de instalação e configuração inicial, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana, a critério exclusivo da CONTRATANTE.

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

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

4.7.3.7. 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, a critério da CONTRATANTE.

4.7.3.8. Para instalação e configuração inicial 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 a ponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da CONTRATANTE, caso a instalação dos produtos / softwares da CONTRATADA apresente falha.

4.7.3.9. 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.

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

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

4.7.3.12. Catálogo de Serviços para Operação Assistida:

I - Para mensuração das quantidades de UST necessárias para execução dos serviços, foi desenvolvido um Catálogo de Serviços relacionando as atividades necessárias e previstas para entrega do objeto, os entregáveis, e as métricas para quantificação dos volumes de serviços necessários para alcance dos objetivos, apresentados na tabela abaixo.

II - Os contratos citados nos subtópicos 2.1.1 e 2.1.2 também foram utilizados como parâmetro para este estudo, através da análise das Ordens de Serviço emitidas durante a execução dos serviços da época.

III - Caso necessário para a implementação e configuração da SOLUÇÃO, será admitida a execução de outras atividades, ficando contudo limitadas ao total contratado de UST.

IV - Os serviços constantes do Catálogo de Serviços, quando necessário, devem contemplar orientações acerca dos cuidados a serem tomados também com dados físicos que possam estar sob guarda do órgão contratante.

V - Os serviços de operação assistida serão demandados de acordo com a necessidade da contratante, mensurados através da métrica de UST, considerando que uma hora de trabalho equivale a uma UST. Ressalta-se, porém, que as medições estarão sempre atreladas ao cumprimento da entrega do produto final (Súmula 269 do TCU, item 8.1.6).

VI - O contrato estabelecerá uma quantidade máxima de UST's a serem utilizadas ao longo de sua vigência, que será representado pelo item 18 da tabela de itens licitados, sendo que a cada emissão de ordem se serviço, o volume será subtraído do quantitativo total disponível. Os serviços poderão se repetir ao longo de toda a vigência do contrato de acordo com a demanda da contratante e até o limite de USTs disponíveis para contratação.

VII - Os serviços de operação assistida indicados no Catálogo de Serviços serão executados de acordo com a especificação indicada em cada item, evidenciado as atividades pormenorizadas para cada um deles, conforme o Catálogo de Serviços. Abaixo, está listado o fator de ponderação de acordo com a complexidade de cada tarefa contida na tabela do catálogo de serviços de forma resumida. A tabela detalhada e demais informações constam do Anexo III - Catálogo de Serviços deste documento:

- São definições dos termos utilizados:
    - Unidade de Serviço Técnico - UST: métrica utilizada para aferir o custo de cada atividade a ser desempenhada;
    - Custo em UST: representa o custo de cada atividade, considerando o tempo de duração em UST e o peso de cada UST; e
    - Duração de UST: tempo de duração para execução de cada atividade, considerando que uma UST tem a duração de 60 minutos.
- A tabela a seguir apresenta o quantitativo de USTs para cada hora de trabalho considerando os respectivos graus de complexidade:

COMPLEXIDADE	FATOR DE PONDERAÇÃO
Baixa	1
Média	2
Alta	3

De acordo com a elevação do nível de complexidade da atividade especificada, é necessário a gradação da especialização do profissional que dará cumprimento a cada rotina da demanda e o ajuste proporcional da UST para a execução de cada item do catálogo.

Catálogo de Serviços (versão resumida)					
ITEM	**DESCRIÇÃO**	**ESFORÇO EM HORAS**	**COMPLEXIDADE**	**FATOR DE PONDERAÇÃO**	**TOTAL DE UST**
1	Projeto Executivo	54	ALTA	3	162
2	Parametrização do Console de Gerenciamento Centralizado	32	ALTA	3	96
3	Parametrização de Agentes	16	MÉDIA	2	160
4	Definição e implementação de procedimentos de backup e restauração do gerenciamento de chaves	24	MÉDIA	2	24
5	Serviço de Apoio Operacional da Solução	120	MÉDIA	2	2.910
				TOTAL	3.322

4.7.4. **Do suporte técnico**

4.7.4.1. A CONTRATADA deverá disponibilizar por meio da Internet, uma aplicação web para registro dos chamados de suporte técnico através de login e senha a ser fornecida para os usuários autorizados pela CONTRATANTE, que deverá operar em regime de 24h x 7 dias, ininterruptamente, inclusive aos sábados, domingos e feriados.

4.7.4.2. A CONTRATANTE poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência da garantia, para suprir suas necessidades com relação à solução contratada.

4.7.4.3. Considera-se "suporte técnico" a prestação de informações, esclarecimentos ou orientações sobre a utilização, funcionalidades (dicas e atalhos), configuração de softwares e hardwares básicos, aplicativos, sistemas da informação em geral envolvidos na solução objeto da contratação, bem como a intervenção direta nos equipamentos para configurações, instalações e remoções de aplicativos, atualizações de softwares e reparos diversos necessários ao bom funcionamento da solução.

4.7.4.4. O suporte técnico deverá contemplar:

I - Manutenção preventiva com vistas a reduzir riscos de problemas futuros, por meio de ações para:

a) garantir que o software opere de maneira eficiente e segura;

b) identificar e resolver possíveis falhas antes que elas possam causar impacto no funcionamento do software.

II - Manutenção corretiva com o objetivo de solucionar defeitos encontrados no software de forma a mantê-lo em pleno funcionamento;

III - Manutenção evolutiva na forma da atualização oportuna das soluções contratadas, empregando 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. A CONTRATADA, durante o prazo contratual, deverá garantir que a solução fornecida esteja sempre atualizada e na última versão disponível. Os acessos para downloads de patches, drivers, e quaisquer outras atualizações de software necessárias, também deverão estar disponíveis no website do fabricante da solução, sem custos adicionais ao CONTRATANTE, durante todo esse período. Manuais técnicos e/ou documentação dos equipamentos e sistemas adquiridos também estarão disponíveis para consulta sempre que necessário;

IV - Manutenção adaptativa na forma da realização das melhorias necessárias de acordo com o ambiente operacional

4.7.4.5. O suporte técnico aqui descrito engloba tanto a prestação de serviço pela CONTRATADA, quanto a responsabilidade desta em acionar o suporte de fabricante da solução, se necessário, não sendo admitido, porém, qualquer dilatação dos prazos para atendimento/solução previstos neste documento.

4.7.4.6. A CONTRATANTE não terá qualquer responsabilidade ou ônus em efetuar contato direto com o suporte do fabricante, devendo a CONTRATADA assumir a total responsabilidade por essa operação, resguardados os prazos do acordo de nível de serviço previsto neste documento.

4.7.4.7. Durante o atendimento, a CONTRATADA poderá analisar a solução, sua atual condição de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica da CONTRATANTE decidirá sobre a aplicação ou não das recomendações.

4.7.4.8. Dentro do prazo contratual, e incluído no escopo do serviço de suporte técnico, a CONTRATADA deverá assegurar que, em caso de constatação de falha física em hardware, um novo equipamento de mesmo part number (ou superior compatível) seja enviado em até 1 (um) dia útil para substituição no ambiente da solução, a partir da comunicação do problema pela CONTRATANTE.

4.7.4.9. Os prazos de atendimento do suporte técnico da solução devem ter como referência os Níveis de Severidade informados na tabela abaixo, ficando a CONTRATADA sujeita às sanções previstas no acordo de nível de serviços previsto neste documento.

TABELA 3			
Severidade	**Descrição**	**Tempo do 1º contato após abertura do chamado**	**Tempo de solução**
alta	Objeto totalmente inoperante	até 1 hora	até 12 horas
média alta	Solução parcialmente inoperante: necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 4 horas	até 24 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 8 horas	até 48 horas
baixa	Solicitações de informações diversas ou dúvidas sobre a solução	até 12 horas	até 72 horas

4.7.4.10. A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi

erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.

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

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

4.7.4.13. Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado, independentemente de este ter sido feito via telefone, e-mail ou website do fornecedor.

4.7.4.14. O serviço de suporte técnico deverá ser prestado em regime 24h x 7 dias, ininterruptamente, inclusive sábados, domingos e feriados.

4.7.4.15. O suporte deverá ser preferencialmente realizado remotamente para solução de problemas, tratamento de falhas, dúvidas e orientações técnicas. Excepcionalmente, quando não for possível de forma remota a resolução do chamado no prazo estabelecido, a CONTRATADA fará o atendimento presencial nas instalações da CONTRATANTE até o completo atendimento da demanda.

4.7.4.16. A CONTRATADA deverá fornecer trimestralmente ao CONTRATANTE, relatório gerencial e relatório técnico com todas as informações sobre os atendimentos realizados, contendo a identificação do problema, providências adotadas e demais informações pertinentes.

4.7.4.17. Os chamados abertos por um órgão CONTRATANTE no sistema de chamados da CONTRATADA não poderão ser visualizados por outros órgãos CONTRATANTES.

4.7.4.18. As disposições sobre Suporte Técnico se aplicam às licenças por aquisição perpétua a título de garantia de produto e também às licenças por subscrição a título de garantia de serviço.

4.7.4.19. 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.

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

4.7.4.21. Não se encaixam nos prazos descritos nos itens referentes aos Níveis de Severidade, 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 Severidade, 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.

4.7.5. **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**

4.7.5.1. As necessidades de mão de obra especializada não dedicada estão diretamente relacionadas com a instalação e configurações (inicial e de operação assistida), suporte técnico da solução e trxeinamento.

4.7.5.2. Considerando a especificidade e a natureza dos serviços a serem prestados, além da obrigação do órgão público em zelar pela adequada utilização dos recursos a ele destinados, faz-se necessário não apenas avaliar a melhor proposta de valor ofertada, mas também a qualificação técnica da proponente que executará os serviços bem como, consequentemente, de seus colaboradores. Tratam-se de serviços de extrema importância que não permitem que empresas sem o “know-how” necessário sejam aceitas no processo licitatório.

4.7.5.3. Por essa razão, a equipe a ser disponibilizada pela CONTRATADA para fins da prestação de todos os serviços aqui descritos deverá ser comprovadamente qualificada, através de certificação na ferramenta em questão, expedida pelo fabricante e com experiência na atividade objeto da contratação.

4.7.5.4. Portanto, além dos atestados citados no tópico 17 a serem apresentados pela proponente como condição para assunção dos serviços, deverão ser fornecidos também,no ato da assinatura do

contrato, os certificados de todos os colaboradores que farão parte das equipes, de modo a comprovar que os mesmos estão aptos à utilização da ferramenta descrita no presente estudo.

4.7.5.5. Serão exigidas cópias simples e individuais dos certificados originais expedidos pelo fabricante da solução a ser ofertada, atestando que os colaboradores estão plenamente treinados e aptos à utilização da aplicação.

4.7.6. **De metodologia de trabalho**

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

a) Ordem de Serviço / Ordem de Fornecimento de bem;

b) Plano de Inserção;

c) Termos de Recebimento;

d) Chamado registrado na Central de Atendimento;

e) Ofícios;Relatórios e Atas de Reunião;

f) E-mail;

g) Demais Termos previstos no instrumento convocatório.

4.7.7.1. A execução de quaisquer dos itens previstos neste estudo será sempre precedida da emissão de Ordem de Serviço/Ordem do Fornecimento de Bem, 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.

4.7.7.2. 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;

4.7.7.3. A comunicação dos usuários com a Central de Atendimento/Suporte da CONTRATADA será realizada por meio de registro de chamado, através de aplicação web, conforme previsto neste documento sobre as condições para suporte técnico.

4.8. **Requisitos Materiais e Humanos**

4.8.1. Materiais, equipamentos, insumos e acessórios necessários ao perfeito funcionamento das soluções componentes do objeto, ainda que após o encerramento do contrato, são de responsabilidade da CONTRATADA.

4.8.2. 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.

4.8.3. **Quantitativo de usuários:**

Não se aplica

4.8.4. **Horário de funcionamento do órgão e horário em que deverão ser prestados os objetos contratados:**

4.8.4.1. O horário de funcionamento do órgão para eventuais serviços de suporte técnico presencial é de 9h às 18h. Para os serviços decorrentes de eventuais emergências, a prestação ocorrerá a qualquer hora do dia, a critério do CONTRATANTE.

4.8.4.2. 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.

4.8.5. Restrições de área, identificando questões de segurança institucional, privacidade, segurança, medicina do trabalho, dentre outras:
Na forma do subtópico 4.6.2. deste documento, no que couber.

4.8.6. **Disposições normativas internas:**

Na forma do subtópico 4.6.2. deste documento.

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

Não se aplica.

4.9. **Fiscalização e Acompanhamento do Contrato**

4.9.1. A execução do contrato será acompanhada e fiscalizada por Comissão de Fiscalização de Contrato da CONTRATANTE, composta na forma do art. 9º do Decreto Estadual nº 48.817/2023.

4.9.2. 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.

4.10. **Metodologia de Avaliação da Qualidade e Aceite do Objeto (ANS)**

4.10.1. Periodicidade: Bimestral.

4.10.2. Início da medição: A partir do 2º mês após a plena instalação e configuração da Solução de Gestão de Chaves Criptográficas (itens 2, 4, 6, 8, 10, 12 e 15).

4.10.3. Mecanismo de cálculo: Somatório dos índices correspondentes aos eventos previstos nas alíneas "a, b, c, d" do subtópico 4.11.19.1deste documento, verificados durante o período.

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

ATENDIMENTO			
SEVERIDADE	**TEMPO MÁXIMO PARA INÍCIO DE ATENDIMENTO**	**TEMPO MÁXIMO PARA SOLUÇÃO OPERACIONAL**	**GRAU DE CUMPRIMENTO**
Crítica	Em até	Em até	95%
Alta	Em até	Em até	95%
Média	Em até	Em até	90%
Baixa	Em até	Em até	85%

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

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

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

4.10.8. O descumprimento deste acordo de nível de serviço, notadamente quanto ao cumprimento dos prazos, ensejará as sanções previstas no subtópico 4.11.19 deste documento.

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

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

4.10.11. Tempo de solução: o tempo de solução de problemas dependerá de sua extensão, gravidade e e risco à disponibilidade ou integridade dos ativos da instituição. A CONTRATADA deverá

fornecer uma estimativa de tempo para solução do problema dentro da primeira hora de atendimento.

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

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

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

4.10.15. 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.

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

4.10.17. A comunicação poderá ser feita pessoalmente, através do preposto designado, ou por meio eletrônico.

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

4.10.19. **Sanções**

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

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

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

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

d) 0,50% do valor anual da solução a título de multa a ser descontado na garantia do contrato, por demanda categorizada como "CRÍTICA" não atendida no prazo, dentro do período de apuração, observados os limites quanto ao início do atendimento e solução operacional.

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

4.11. **Indicação de marca (ou modelo) e vedação de utilização de marca (quando cabível)**

Não aplicável ao objeto em estudo.

5. LEVANTAMENTO DE MERCADO

5.1. Levantamento das Soluções

Solução 1 - Utilização de ferramentas Open Source (uso gratuito)

Utilização de soluções criptográficas de código aberto. Neste caso, seria necessário um conjunto de softwares open source para desempenhar as funcionalidades necessárias ao atendimento da demanda;

- Vantagens: Por conta das ferramentas gratuitas e disponíveis na internet, esta opção não envolve

custos diretos com a contratação da solução e possibilita uma customização dos softwares.
- Desvantagens: Riscos de descontinuidade do(s) software(s); ausência de suporte técnico especializado; curva de experiência da equipe de trabalho para o pleno domínio da operacionalização do(s) software(s); impossibilidade de um gerenciamento centralizado. São necessárias diversas ferramentas open source para desempenhar as funcionalidades de uma solução corporativa/enterprise. Ainda assim, tal operação seria algo complexo e desconexo, e os relatórios de inteligência, justamente por estarem difusos entre várias soluções, não possuiriam a mesma assertividade daqueles oriundos de uma ferramenta capaz de centralizar o resultado do monitoramento de diversas fontes de dados. Haveria ainda a necessidade de o órgão contratante operar tais soluções gratuitas, correlacionado os dados de inteligência produzidos, de maneira a manter a infraestrutura de tal solução, o que implicaria em designar quadros técnicos especializados para a operação e manutenção da solução, sem a garantia de uma perfeita integração com a solução atualmente em uso e sem a possibilidade de um suporte técnico eficiente ou mesmo efetivo.

Solução 2 - Criação de uma solução sob demanda pelo órgão contratante, ou utilizando a Gerência de Fábrica de Software/PRODERJ para o desenvolvimento da solução.

Neste caso o PRODERJ desenvolveria uma solução de gestão de chaves criptográficas e anonimização de dados. No entanto, tal cenário seria viabilizado apenas caso houvesse grande investimento em treinamento e contratações para a equipe de desenvolvimento, atividades que demandam o emprego de tempo e recursos financeiros.

- Vantagens: Propriedade sobre o desenvolvimento, sem a necessidade de custo com licenciamentos; gestão própria da solução; maior aderência às necessidades específicas do órgão contratante.
- Desvantagens: Curva de experiência e maturação de longo prazo para o preparo dos quadros técnicos da casa para a elaboração de uma ferramenta similar a que está em utilização atualmente; tempo para o desenvolvimento dessa solução seria de longo prazo; ausência de know-how técnico da equipe da casa para o desenvolvimento de soluções de segurança da informação; aplicabilidade defasada em função da volatilidade de soluções tecnológicas e aplicações; o investimento, a priori, não se aplicaria tão somente à solução em si, mas a todo o arcabouço técnico e humano necessários para o desenvolvimento da solução.

Solução 3 - Consultorias e Serviços Gerenciados

Empresas de consultoria em segurança cibernética, como Deloitte, PwC e Accenture, podem oferecer serviços personalizados para anonimização de dados e gerenciamento de chaves, ajudando na implementação de soluções adequadas às necessidades específicas da organização.

Vantagens:

- Expertise Especializada: consultorias possuem equipes de especialistas com profundo conhecimento em segurança da informação, compliance e melhores práticas de anonimização de dados. Isso pode garantir que as soluções implementadas estejam alinhadas com as normas e regulamentos aplicáveis;
- Soluções Personalizadas: as consultorias podem desenvolver soluções sob medida que atendam às necessidades específicas da organização, considerando seus processos, infraestrutura e requisitos de conformidade;
- Avaliação de Risco: oferecem uma análise abrangente dos riscos associados à proteção de dados, ajudando a identificar vulnerabilidades e a implementar medidas adequadas para mitigá-las;

Desvantagens

- Custo Elevado: serviços de consultoria e gerenciamento podem ser significativamente mais caros do que soluções de software ou plataformas em nuvem, especialmente para pequenas e médias empresas;
- Dependência Externa: a contratação de serviços gerenciados pode criar uma dependência em relação à consultoria, o que pode ser problemático se a relação não for mantida ou se houver mudanças na equipe da consultoria;
- Tempo de Implementação: o processo de análise, planejamento e implementação pode ser demorado, especialmente em organizações grandes ou com estruturas complexas;
- Possíveis Conflitos de Interesse: algumas consultorias podem ter parcerias com fornecedores específicos, o que pode influenciar suas recomendações e levar a uma falta de imparcialidade na

escolha das melhores soluções;
- Complexidade de Integração: a implementação de soluções personalizadas pode envolver complexidades de integração com sistemas existentes, o que pode exigir mais tempo e recursos.
- Suporte Contínuo: oferecem serviços gerenciados que incluem suporte contínuo e monitoramento, garantindo que as soluções permaneçam eficazes e atualizadas frente a novas ameaças;
- Treinamento e Capacitação: podem oferecer treinamento para equipes internas, capacitando-as a gerenciar e manter as soluções de anonimização e gerenciamento de chaves de forma eficaz.

Solução 4 - Contratação de empresa especializada no Fornecimento/licenciamento de Solução de Anonimização de Dados e Gerenciamento de Chaves Criptográficas.

Neste caso, haveria a contratação de uma única empresa especializada de modo a disponibilizar a cobertura de anonimização em menor tempo aos sistemas hospedados, sobretudo diante das exigências da LGPD.

- Vantagens: Aplicações e ferramentas de mercado devidamente alinhadas à realidade da tecnologia atual; maior celeridade na implementação do projeto e alcance dos benefícios esperados, em comparação, inclusive, com a Solução 3; melhor eficiência em relação à utilização de corpo técnico, podendo direcionar os recursos humanos para gestão do processo e desenvolvimento de novos projetos; custo reduzido de capacitação e energia em relação à contratação de profissionais com background específico para desenvolvimento; soluções compostas por um único fornecedor tendem a abranger uma gama maior de informações e garantir maior agilidade no atendimento aos objetivos relacionados à conformidade com a Lei 13.709 – Lei Geral de Proteção de Dados e demais padrões de segurança recomendados para órgãos da administração pública; maior aderência de plataforma de mercado ao atendimento às normas regulatórias e legais relacionadas com a continuidade dos negócios e responsabilidade civil do administrador de T.I..
- Desvantagens: Dependência de tecnologias externas (em comparação com a Solução 3); ciclo contínuo de investimento na contratação e manutenção da solução; necessária contratação de suporte técnico continuado; riscos associados à dinâmica de mercado dos fabricantes de tecnologia e suas revendas autorizadas.

6. ANÁLISE DE PROJETOS SIMILARES

6.1. Na tabela a seguir, a análise qualitativa de contratações similares:

ÓRGÃO / ENTIDADE		Nº Contrato / Edital	Valor (R$)	Fornecedor	Natureza do Objeto	Período de subscrição / garantia do produto	ANÁLISE DA CONTRATAÇÃO
01	Prefeitura de João Pessoa - PB	P.E. SRP nº 6.003/2024, ARP nº 13/2024 e Contrato nº 6693/2024 (94074040)	20.290.266,00	ARS Tecnologia Serviços e Consultoria Ltda	aquisição de bens junto com serviços	12 meses	Objeto composto de lote único contemplando licenças de aquisição perpétua, licenças temporárias (subscrição), com serviços de suporte técnico, de operação assistida e de treinamento. O serviço de Operação Assistida foi contratado por unidade mensal de serviço. (aplicado Sistema de Registro de Preços)

02	PRODERJ	P.E. nº 07/2022 ARP nº 001/2023 Contratos 025 e 026/2023 Contrato 007 e 008/2024 (84324069)	13.837.609,00	ARS Tecnologia Serviços e Consultoria Ltda	aquisição de bens junto com serviços	12 meses	Plataforma implementada e em operação no PRODERJ, com escopo para atendimento de até 35 sistemas/bancos de dados. Objeto composto de lote único contemplando licenças de aquisição perpétua, licenças temporárias (subscrição), com serviços de suporte técnico, de operação assistida e de treinamento. O serviço de Operação Assistida foi contratado por unidade de UST. (aplicado Sistema de Registro de Preços)
03	DETRAN RJ	P.E. nº 06/2022 Contrato nº 37/2023 (84327402)	9.740.000,00	ARS Tecnologia Serviços e Consultoria Ltda	aquisição de bens junto com serviços	12 meses	Objeto composto de lote único contemplando licenças de aquisição perpétua, licenças temporárias (subscrição), com serviços de suporte técnico, de operação assistida e de treinamento. O serviço de Operação Assistida foi contratado por unidade mensal de serviço.
04	CET SP	P.E. nº 028/2022 e Contrato nº 73/2022 - expirado em 2023 (94106216)	13.805.480,00	ARS Tecnologia Serviços e Consultoria Ltda	aquisição de bens junto com serviços	24 meses	Objeto composto de lote único contemplando licenças de aquisição perpétua, licenças temporárias (subscrição), com serviços de suporte técnico, de operação assistida e de treinamento. O serviço de Operação Assistida foi contratado por unidade mensal de serviço. (não aplicado o Sistema de Registro de Preços)

7. MÉTRICAS PARA MENSURAÇÃO DOS SERVIÇOS

7.1. Adoção da métrica UST no item de Operação Assistida

7.1.1. Propõe-se a adoção da métrica UST para o serviço especializado sob demanda de operação assistida como parâmetro de demanda, bem como para avaliar critérios de aferição de pagamento por resultado.

7.1.2. UST - Unidade de Serviço Técnico é unidade de medição de trabalho que envolve esforço humano não mensurável previamente de forma precisa, sendo amiúde utilizada em contratos de prestação de serviços que envolvem diversas tarefas com variações de complexidade e costuma ser observada em contratações públicas relacionadas aos objetos tecnológicos.

7.1.3. A métrica coaduna com o caráter de requisição de operação assistida, sob demanda.

I - Vantagens:

a) A UST está diretamente ligada aos resultados entregues, ou seja, às funcionalidades e serviços efetivamente prestados.

b) A utilização da UST permite um planejamento mais preciso dos projetos, facilitando a estimativa de custos e prazos.

c) A UST é definida com base em um catálogo de serviços (vide item 4.8.3.3. deste documento), com especificações claras sobre o que cada unidade representa, elaborado conforme as boas práticas observadas da SGD/MGI nº 750/2023. Isso facilita a compreensão e a interação entre as partes envolvidas no contrato para fins de emissão de Ordens de Serviços.

d) A métrica UST facilita a auditoria dos contratos, permitindo verificar se os serviços contratados foram realmente entregues.

e) Flexibilidade para adaptar a métrica a diferentes tipos de serviços e projetos.

f) Permite uma avaliação mais detalhada do esforço necessário para cada tarefa.

II - Desvantagens:

a) Complexidade na elaboração do contrato, uma vez que exigiria maior esforço no planejamento para que as unidades de medida fossem adequadas e refletissem a realidade dos serviços e a exigência de um acompanhamento rigoroso, de forma a garantir que os serviços sejam prestados de acordo com o que foi pactuado.

7.1.4. Uma alternativa ao uso de UST é a contratação como serviço mensal, nos moldes observados no contrato do DETRAN RJ (vide tabela do subtópico 6.1. deste documento).

7.1.5. Todavia, a modalidade não é aplicável ao objeto proposto neste documento, uma vez que se apresenta como componente de uma solução composta de diversos softwares, sendo licitado em Sistema de Registro de Preços.

7.1.6. No cenário proposto pelo PRODERJ, que atenderá múltiplos órgãos, a métrica UST viabiliza a compatibilização da demanda a partir de uma unidade padronizada de métrica.

7.1.7. No exemplo observado do DETRAN não havia essa situação, uma vez que aquele órgão não fez licitação em SRP e pôde definir todos os itens a compor o seu modelo de plataforma de anonimização de dados, bem como as respectivas quantidades, viabilizando assim, por parte dos licitantes, o dimensionamento dos serviços a serem prestados ao longo de 12 meses, e estabelecendo um valor mensal fixo.

7.1.8. A título de referência, observe-se alguns entendimentos acerca do uso da UST, já assentados pelo Egrégio Tribunal de Contas da União, constantes na Súmula 269, in verbis:

> " Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos.
>
> Fundamento legal:
>
> - Constituição Federal, art. 37, caput;
>
> - Decreto nº 2.271/97, art. 3º, § 1º. "

7.1.9. Por fim, a escolha da Unidade de Serviço Técnico (UST) em contratações de Tecnologia da Informação (TI) para a administração pública pode trazer diversos benefícios. Aqui estão alguns deles:

7.1.10. Padronização: A UST oferece uma medida padronizada para estimar o esforço necessário

para a realização de um serviço ou projeto de TI. Isso permite comparar propostas de diferentes fornecedores de maneira mais objetiva, evitando discrepâncias na interpretação de outras unidades de medida.

7.1.11. Simplificação: A UST simplifica o processo de contratação, pois elimina a necessidade de detalhar todas as atividades e tarefas envolvidas em um projeto. Em vez disso, o foco está no resultado final esperado, medido em UST. Isso reduz a complexidade e a burocracia do processo de aquisição.

7.1.12. Flexibilidade: A UST permite maior flexibilidade na definição dos requisitos e na adaptação durante o desenvolvimento do projeto. As unidades de medida tradicionais, como horas de trabalho ou custo por hora, podem ser menos flexíveis, pois estão vinculadas a uma abordagem mais rígida de gerenciamento de projetos.

7.1.13. Transparência: A UST pode aumentar a transparência no processo de contratação, pois facilita a compreensão dos custos envolvidos e dos esforços necessários. As partes envolvidas podem ter uma visão clara do valor entregue em relação ao custo.

7.1.14. Comparabilidade: A adoção da UST permite a comparação direta de diferentes propostas de fornecedores, uma vez que todos estão utilizando a mesma unidade de medida. Isso facilita a análise das propostas e a tomada de decisão, levando em consideração tanto o custo quanto o escopo do projeto.

7.1.15. Controle de custos: A UST facilita o controle de custos durante a execução do projeto, pois é uma medida direta do esforço envolvido. Isso pode ajudar a evitar custos excessivos e garantir um melhor gerenciamento financeiro.

8. DEFESA DE MARCA

8.1. Não aplicável ao objeto em estudo.

9. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

9.1. Observadas as soluções de mercado apontadas no tópico 5 deste documento, a Solução 4 se apresenta como a mais adequada tecnicamente, indicando o melhor custo/benefício.

9.2. Tal solução aponta para modelo de contratação de empresa especializada no fornecimento de licenças de softwares e serviços agregados voltados à implementação de uma plataforma de anonimização de dados.

9.3. Em relação à Solução 01, a solução escolhida oferece condições de suporte e manutenção, mediante atribuição de responsabilidade e de garantia, bem como oferece estabilidade e continuidade no uso da solução de forma segura. Em relação à Solução 2, ela é mais dinâmica por ser uma solução pronta e não envolver todo um processo de desenvolvimento de software(s) para o atendimento da demanda. Em relação à Solução 3, esta configura-se como menos vantajosa, tendo em vista a total dependência tecnológica do CONTRATADO, desafios elevados para integração com sistemas existentes, tempo elevado para sua implementação. Saliente-se tratar de modelo de solução já em execução no PRODERJ e outros órgãos da Administração (vide subtópico 2.1.5 deste documento).

9.4. Ademais, a terceirização da solução tende a permitir que a equipe interna do CONTRATANTE se concentre nas atividades principais da organização, em vez de se dedicar ao desenvolvimento e manutenção de um software complexo.

9.5. Em resumo, a opção por licitar uma empresa especializada oferece segurança, conformidade legal, redução de custos a longo prazo e eficiência operacional, enquanto soluções próprias ou gratuitas podem trazer riscos técnicos, jurídicos e financeiros. A escolha por um fornecedor qualificado garante uma implementação rápida, robusta e alinhada às melhores práticas do mercado.

10. ESTIMATIVAS DAS QUANTIDADES A SEREM CONTRATADAS

10.1. Tendo em vista que o presente estudo está sendo desenvolvido para o atendimento de pedido encaminhado por outros órgãos da Administração (vide item 1.3. deste documento) e que não há expectativa de contratação da solução em estudo pelo PRODERJ, os quantitativos estimados para contratação serão apurados em fase de Intenção de Registro de Preços (IRP).

Nº do Item	ID SIGA	Descrição do Bem ou Serviço	Métrica	Quantidade estimada (a apurar, conforme subtópico 10.1)	Mecanismos de quantificação da demanda
1	169955	CONSOLE DE GERENCIAMENTO centralizado em alta disponibilidade, incluindo licenciamento permanente, instalação e configuração	Unidade	2	Aquisição de uma unidade por contratante, acrescido de outra unidade a título de redundância (alta disponibilidade) para fins de resguardo contra incidentes cibernéticos;
2	169956	Serviço de manutenção, atualização de versão e garantia para CONSOLE DE GERENCIAMENTO	Serviço	2	A quantidade corresponde à mesma demandada para o item 1.
3	169957	AGENTES DE PROTEÇÃO DADOS PARA BANCO DE DADOS, incluindo licenciamento permanente, instalação e configuração	Unidade	10	Aquisição de uma unidade por servidor de banco de dados na infraestrutura do CONTRATANTE
4	169958	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DADOS PARA BANCO DE DADOS	Serviço	10	A quantidade corresponde à mesma demandada para o item 3.
5	169959	AGENTES PARA COMPARTILHAMENTO SEGURO DE BASE DE DADOS, incluindo licenciamento permanente, instalação e configuração	Unidade	1	Aquisição de uma unidade por ambiente/rede na infraestrutura do CONTRATANTE
6	169960	Serviço de manutenção, atualização de versão e garantia para AGENTES PARA COMPARTILHAMENTO SEGURO DE BASE DE DADOS	Serviço	1	A quantidade corresponde à mesma demandada para o item 5.
7	169961	AGENTES DE PROTEÇÃO DE DADOS PARA SERVIDORES DE ARQUIVO (FILE SERVER), incluindo licenciamento permanente, instalação e configuração	Unidade	7	Aquisição de uma unidade por host (S.O) na infraestrutura do CONTRATANTE
8	169962	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DE DADOS PARA SERVIDORES DE ARQUIVO (FILE SERVER)	Serviço	7	A quantidade corresponde à mesma demandada para o item 7.
9	169963	AGENTES DE PROTEÇÃO DE DADOS PARA CONTÊINERES, incluindo licenciamento permanente, instalação e configuração	Unidade	15	Aquisição de uma unidade por servidor de contêineres na infraestrutura do CONTRATANTE
10	169964	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DE DADOS PARA CONTÊINERES	Serviço	15	A quantidade corresponde à mesma demandada para o item 9.
11	169965	AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO, incluindo licenciamento permanente, instalação e configuração	Unidade	21	Aquisição de uma unidade por aplicação na infraestrutura do CONTRATANTE
12	169966	Serviço de manutenção, atualização de versão e garantia para AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO	Serviço	21	A quantidade corresponde à mesma demandada para o item 11.
13	170934	Subscrição de agentes para gestão de chaves na nuvem, incluindo instalação e configuração - Termo de licenciamento por 12 (doze) meses	Unidade	2	uma unidade por aplicação em nuvem na infraestrutura do CONTRATANTE
14	169969	AGENTES PARA GESTAO DE CHAVES LOCAL, incluindo licenciamento permanente, instalação e configuração	Unidade	2	Aquisição de uma unidade por cliente de criptografia nativa

15	169970	Serviço de manutenção, atualização de versão e garantia para AGENTES PARA GESTAO DE CHAVES LOCAL	Serviço	2	A quantidade corresponde à mesma demandada para o item 14.
16	170384	Subscrição de agentes para descoberta e classificação de dados, incluindo instalação e configuração. Termo de Licenciamento por 12 (doze) meses (Franquia 50 TB)	Unidade	1	Uma unidade por franquia de 50TB
17	169975	Serviço de treinamento para solução de gerenciamento de chaves criptográficas	Vaga (aluno)	6	A quantidade corresponde ao quantitativo de funcionários da CONTRATANTE a serem treinados na solução, considerados aqueles cuja atividade está diretamente relacionada à aplicação ou operacionalização das ferramentas de segurança cibernética. (ITEM SOB DEMANDA). O PRODERJ, a título de exemplo, considerou a possibilidade de treinamento de 3 funcionários da área de infraestrutura e 3 funcionários da área de segurança da informação.
18	170683	Serviço de operação assistida para solução de gerenciamento de chaves criptográficas	UST	3.322	A quantidade corresponde a uma expectativa mínima de ocorrência das atividades previstas no Catálogo de Serviços ao longo de um período de 12 (doze) meses que correspondem à duração dos serviços de manutenção da solução. (ITEM SOB DEMANDA). O PRODERJ, a título de exemplo, considerou uma expectativa de até 3 ocorrências para cada atividade ao longo de 12 meses.

11. ESTIMATIVA PRELIMINAR DO VALOR DA CONTRATAÇÃO

11.1. A estimativa preliminar do valor da contratação apresentada na tabela abaixo, visando uma análise comparativa quanto à viabilidade econômica da solução escolhida neste estudo técnico, considerou os parâmetros observados nos certames e contratações similares realizadas por outros órgãos, inclusive pelo próprio PRODERJ

11.2. 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 existe para esses produtos, dentre os catálogos de soluções de TIC com condições padronizadas publicados pelo Governo Federal,

11.3. nenhum referente à solução "Anonimização de Dados e Gerenciamento de Chaves Criptográficas" ou similar que pudesse ser utilizado o preço de referência.

11.4. Uma vez que a estimativa de quantidades a serem contratadas serão apuradas em procedimento de Intenção de Registro de Preços (IRP) em fase posterior, a estimativa preliminar do valor da contratação abaixo demonstrada, considera a contratação de ao menos uma unidade de cada item previsto no lote, excetuado o de serviço de operação assistida, com medição por UST, cujo parâmetro utilizado foi a demanda contratada pelo PRODERJ em seu contrato realizado em 2023.

Nº do Item	ID SIGA	Descrição do Bem ou Serviço	Métrica	Qtde. Estimada	Prefeitura de João Pessoa - PB (R$ - valor unitário)	Contrato PRODERJ (R$ - valor unitário) +4,68% reajuste concedido (76525466)	Contrato DETRAN RJ (R$ - valor unitário) + 1.17% reajuste concedido (73821453)	CET SP (R$ - valor unitário)	PRODAM-SP (R$ valor unitário)	Valor médio Unitário (mensal)	Valor Total estimado (12 meses)
1	169955	CONSOLE DE GERENCIAMENTO centralizado em alta disponibilidade, incluindo licenciamento permanente, instalação e configuração	Unidade	2	911.125,00 (licença perpétua)	631.398,36	610.227,09	473.500,00 (licença perpétua)	743.789,50	674.007,99	1.348.015,98
2	169956	Serviço de manutenção, suporte técnico e atualização de versão para CONSOLE DE GERENCIAMENTO	Serviço	2	32.650,00 (mensalidade)	137.995,46(ano) Mensal = 11.499,62	62.725,40 (mensalidade) Valor descartado	11.425,00 (mensalidade)	168.024,00 (ano) Mensal 14.002,00	13.915,32	333.967,68
3	169957	AGENTES DE PROTEÇÃO DADOS PARA BANCO DE DADOS, incluindo licenciamento permanente, instalação e configuração	Unidade	10	242.000,00 (licença perpétua)	144.387,22	não demandado	118.300,00 (licença perpétua)	não demandado	168.229,07	1.682.290,73
4	169958	Serviço de manutenção, suporte técnico e atualização de versão para AGENTES DE PROTEÇÃO DADOS PARA BANCO DE DADO	Serviço	10	23.850,00 (mensalidade)	26.567,78 Média mensal = 2.213,98	não demandado	6.250,00 (mensalidade)	não demandado	10.771,33	1.292.559,60
5	169959	AGENTES PARA COMPARTILHAMENTO SEGURO DE BASE DE DADOS, incluindo licenciamento permanente, instalação e configuração	Unidade	1	749.975,00 (licença perpétua)	573.646,40	554.411,60	503.400,00 (licença perpétua)	576.200,00	591.526,60	591.526,60
6	169960	Serviço de manutenção, suporte técnico e atualização de versão para AGENTES PARA COMPARTILHAMENTO SEGURO DE BASE DE DADOS	Serviço	1	14.020,00 (mensalidade)	96.077,40 Média mensal= 8.006,45	7.737,99 (mensalidade)	5.353,00 (mensalidade)	123.240,00 (ano) Mensal: 10.270,00	9.077,48	108.929,76

7	169961	AGENTES DE PROTEÇÃO DE DADOS PARA SERVIDORES DE ARQUIVO (FILE SERVER), incluindo licenciamento permanente, instalação e configuração	Unidade	7	229.122,00 (licença perpétua)	103.737,88	100.259,47	104.130,00 (licença perpétua)	176.334,00	142.716,67	999.016,69
8	169962	Serviço de manutenção, suporte técnico e atualização de versão para AGENTES DE PROTEÇÃO DE DADOS PARA SERVIDORES DE ARQUIVO (FILE SERVER)	Serviço	7	7.970,00 (mensalidade)	24.897,09 Mensal = 2.074,76	30.077,84 (mensalidade) Valor descartado	13.048,00 (mensalidade)	37.656,00 Mensal: 3.138,00	5.246,15	440.676,76
9	169963	AGENTES DE PROTEÇÃO DE DADOS PARA CONTÊINERES, incluindo licenciamento permanente, instalação e configuração	Unidade	15	não demandado	126.662,80	não demandado	não demandado	não demandado	126.662,80	1.899.942,00
10	169964	Serviço de manutenção, suporte técnico e atualização de versão para AGENTES DE PROTEÇÃO DE DADOS PARA CONTÊINERES	Serviço	15	não demandado	28.054,24	não demandado	não demandado	não demandado	28.054,24	5.049.763,2
11	169965	AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO, incluindo licenciamento permanente, instalação e configuração	Unidade	21	não demandado	159.347,04	154.004,01	não demandado	196.810,00	166.709,14	3.500.892,04
12	169966	Serviço de manutenção, suporte técnico e atualização de versão para AGENTES DE PROTEÇÃO DE DADOS PARA APLICAÇÃO	Serviço	21	não demandado	29.902,89 Mês = 2.491,91	12.041,76 (mensalidade)	não demandado	41.758,80 Mensal: 3.479,90	6.004,52	1.513.139,04

13	170934	Subscrição de agentes para gestão de chaves na nuvem, incluindo instalação e configuração - Termo de licenciamento por 12 (doze) meses	Serviço	2	não demandado	615.518,40	não demandado	não demandado	não demandado	615,518,40	1.231.036,80
14	169969	AGENTES PARA GESTÃO DE CHAVES LOCAL, incluindo licenciamento permanente, instalação e configuração	Unidade	2	54.500,00 (licença perpétua)	15.702,00	não demandado	não demandado	não demandado	54.500,00	109.000,00
15	169970	Serviço de manutenção, suporte técnico e atualização de versão para AGENTES PARA GESTÃO DE CHAVES LOCAL	Serviço	2	1.588,00 (mensalidade)	2.595,02	não demandado	não demandado	não demandado	2.091,51	50.196,24
16	170384	Subscrição de agentes para descoberta e classificação de dados, incluindo instalação e configuração. Termo de licenciamento por 12 (doze) meses (franquia 50 TB)	Serviço	1	150.806,00 (mensalidade)	1.155.667,20 Mês = 96.305,60	não demandado	86.222,00 (mensalidade)	não demandado	111.111,20 Valor ano =	1.333.334,40
17	169975	Serviço de treinamento para solução de gerenciamento de chaves criptográficas	Unidade	6	92.500,00 (turma de até 10 vagas) Valor aluno= 9.250,00	5.234,00 (por aluno)	68.795,60 (por turma) Valor descartado	47.000,00 (turma de até 10 vagas) Valor aluno = 4.700,00	60.580,00 (turma de até 10 vagas) Valor aluno = 6.058,00	6.310,5	37.863,00
18	170683	Serviço de operação assistida para solução de gerenciamento de chaves criptográficas	UST	3.322	267.527,00 (mensalidade)	438,00	92.000,00 (mensalidade)	63.500,00 (mensalidade)	99.030,00 (mensalidade)	Por UST = 438,00	1.455.036,00
Valor estimado da futura contratação											**22.637.206,52**

12. DESCRIÇÃO DA SOLUÇÃO DE TI COMO UM TODO

12.1. Contratação de empresa para a aquisição de console de gerenciamento, agentes de proteção de dados para banco de dados, agentes para compartilhamento seguro de base de dados, agentes de proteção de dados para servidores de arquivo (file servers), agentes de proteção de dados para contêineres, agentes de proteção de dados para aplicação, agentes para gestão de chaves local, e prestação dos serviços de plataforma de anonimização e gerenciamento de chaves criptográficas, controle de acesso, visibilidade e rastreabilidade de utilização de dados em servidores de arquivos, banco de dados, infraestrutura em nuvem (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS), incluindo serviço de instalação, configuração da solução, integrações necessárias com soluções de terceiros e serviços especializados, conforme Anexo I (Especificações Técnicas do Objeto) deste documento, bem como treinamentos operacionais das soluções contratadas, voltados para os técnicos da CONTRATANTE, conforme especificações e quantidades estabelecidas no Termo de Referência e nos requisitos da contratação descritos nestes Estudos Técnicos Preliminares.

12.2. A empresa contratada, fornecedora das licenças de uso perpétuo, deverá fornecer

garantia de no mínimo 1 (um) ano, contado a partir do recebimento definitivo do objeto, de acordo com as normas vigentes, pelo qual se obriga, independentemente de ser ou não o fabricante do(s) produto(s), a efetuar a qualquer tempo, substituições de todas as unidades que apresentarem defeitos de fabricação sem ônus para o órgão contratante, desde que estes não sejam provenientes de operação ou manuseio inadequado após a entrega.

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, observados os seguintes aspectos:

a) Os itens 1, 3, 5, 7, 9, 11 e 14 são licenças perpétuas de software, medidas em unidades;

b) Os itens 2, 4, 6, 8, 10, 12 e 15 são serviços contínuos de manutenção, suporte, atualização e garantia, relativos respectivamente aos itens da alínea anterior, medidos em unidades;

c) Os itens 13 e 16 são licenças por subscrição de software, com natureza de serviço contínuo, medidos em unidades;

d) O item 17 é serviço de treinamento, sob demanda, medido por vaga/aluno;

e) O item 18 do lote é serviço sob demanda de Operação Assistida, com natureza contínua e medido por Unidade de Serviço Técnico - UST.

14. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

14.1. O parcelamento do objeto não é técnica e economicamente viável, 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.

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. Recomenda-se que a solução advenha de fornecedor único, para que seus componentes, módulos e/ou programas sejam totalmente integrados entre si. Desta forma, teremos as seguintes vantagens:

I - Integração total entre os módulos que compõem o software da solução;

II - Gerenciamento centralizado em apenas uma solução;

III - Simplificação na gestão de logs e análises de tentativas de invasão;

IV - Redução com custo de manutenções e configurações quotidianas, como correções de segurança e atualizações de versões.

14.4. Pela natureza do objeto, enquanto solução integrada de múltiplas funcionalidades e, sendo a mitigação de pontos de falha e vazamento de dados objetivos indispensáveis desta licitação, o fracionamento do objeto distribuindo-o em parcelas torna-se notadamente inviável, sob pena desta Administração incorrer nos fatos abaixo indicados:

I - Em caso de eventual exposição de dados sigilosos não será possível precisar de qual módulo se originou a falha, permitindo que as empresas transfiram a responsabilidade para terceiros, impedindo assim a penalização legal pelo fato ocorrido e a avaliação dos pontos de mitigação;

II - Fracionar o objeto em módulos potencializará riscos inerentes a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), pois permitirá que a gestão dos módulos seja feita por mais de uma empresa, e o controle, a análise, a manutenção e o gerenciamento de acessos e a veiculação de dados será notadamente exposto a um número significativo de agentes, colaboradores e gestores de contrato, aumentando o risco de vazamentos;

III - Caso o objeto seja parcelado em vários lotes, haverá vários softwares redundantes executando as mesmas funções. Serão necessários, portanto, recursos humanos e tecnológicos para operacionalizar cada uma dessas hipotéticas soluções; e ainda assim, esta operacionalização ocorrerá de forma fragmentada e o risco de acarretar incompatibilidade entre as soluções é extremo.

14.5. O objeto compreende a instalação, treinamento, manutenção e implementação dos agentes e módulos, exigindo que funcionem de forma integrada e indissociável. Dessa forma, o fracionamento certamente ocasionará uma perda significativa de eficiência durante todos os processos indicados, onerando a CONTRATANTE com a perda de celeridade do processo de implantação da solução.

14.6. O agrupamento dos itens levou em consideração questões técnicas e ganho de economia em escala, sem prejuízo à ampla competitividade. Há várias empresas no mercado com capacidade de fornecer os produtos e serviços na forma em que estão agrupados neste documento, onde conferirá, ainda, a execução e a fiscalização do contrato com um maior nível de controle pela Administração, sendo prática comum reconhecida pelo mercado.

14.7. Desse modo, a indissociabilidade do objeto justifica-se, uma vez que preserva os objetivos da futura contratação e garante maior eficiência sobre a execução e gestão do contrato, garantindo a adequação à Lei Geral de Proteção de Dados Pessoais (LGPD) e mitigando riscos associados ao vazamento de dados dessa Administração.

14.8. O objeto ora pretendido se configura em uma solução de TI composta por itens variados de naturezas distintas (aquisição de software, serviços manutenção e suporte, de treinamento e de subscrição de licença de software), todos com as suas funcionalidades a serem desempenhadas de forma unificada e administrada em conjunto, portanto, em plena interoperabilidade técnica e operacional.

14.9. O agrupamento dos itens permite uma gestão mais eficiente do ambiente de TI, não apenas no âmbito da funcionalidade da solução, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, a resolução de conflitos entre fornecedores distintos. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado, não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, as configurações, o suporte técnico e o treinamento serão executados por um único fornecedor e prestador de serviços.

14.10. Dessa forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores.

14.11. Assim, entende-se que é fundamental para a pretensa contratação, e necessário para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que todos os itens ora propostos sejam adquiridos/contratados de forma agrupada, conforme proposto, em lote único.

14.12. Dividir o objeto entre fornecedores distintos ocasionará prejuízos técnicos, como também riscos de danos tecnológicos, visto que a manutenção, a garantia, o suporte técnico e o treinamento, se realizados por vários fornecedores, exigindo um tempo excessivo, ou até mesmo impossibilitando dirimir divergências entre possíveis incompatibilidades, causando um potencial risco de operacionalização e funcionamento, pela adoção de procedimentos variados ou divergentes.

14.13. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado, resguardada da compatibilidade operacional entre os elementos de hardware, melhor gerenciamento do contrato e obtenção dos serviços de suporte e treinamento.

14.14. Em suma, a opção pelo fornecimento por grupo de itens leva em conta a modalidade de contratação pretendida e os benefícios associados. Tal agrupamento não compromete a competitividade do certame, uma vez que várias empresas que atuam no mercado apresentam condições para cotar os itens pretendidos para a futura contratação apresentada neste documento.

14.15. Portanto, a opção pelo modelo de contratação de empresa única para o fornecimento de solução pronta considera os seguintes aspectos:

14.16. Expertise e Conformidade Legal: Empresas dedicadas à anonimização de dados

possuem experiência comprovada em técnicas avançadas (como pseudonimização, k-anonimidade, diferencial de privacidade, etc.), garantindo maior eficácia na proteção dos dados;

14.17. Proteção contra vulnerabilidades: Desenvolver uma solução interna exige testes rigorosos para evitar brechas que possam comprometer dados sensíveis. Um fornecedor especializado já oferece soluções validadas pelo mercado;

14.18. Atualizações contínuas: Empresas terceirizadas mantêm seus sistemas atualizados contra novas ameaças cibernéticas, enquanto soluções próprias ou gratuitas podem ficar defasada;

14.19. Economia de tempo e recursos: Desenvolver um software robusto demandaria investimento em equipe qualificada (cientistas de dados, desenvolvedores, especialistas em segurança), além de tempo para testes e implementação;

14.20. Manutenção simplificada: Soluções terceirizadas incluem suporte técnico, enquanto soluções internas exigiriam custos contínuos de manutenção;

14.21. Adaptação a diferentes volumes de dados: Soluções profissionais são projetadas para escalar conforme a necessidade, enquanto soluções próprias podem exigir refatoração constante;

14.22. Integração com sistemas existentes: Ferramentas de fornecedores especializados geralmente oferecem compatibilidade com bancos de dados, ERPs e outras plataformas utilizadas pela organização;

14.23. Falta de suporte e personalização: Ferramentas open-source ou gratuitas podem não atender requisitos específicos da organização ou não ter suporte em caso de falhas;

14.24. Riscos de compliance: Muitas soluções gratuitas não possuem certificações ou garantias de conformidade com leis de proteção de dados.

15. RESULTADOS PRETENDIDOS

15.1. 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) Proteger as informações contra acessos e distribuições não autorizados;

b) Elevar o nível de confiabilidade dos sistemas;

c) Garantir a segurança e a disponibilidade dos serviços prestados;

d) Promover compartilhamento seguro dos dados;

e) Prevenir e minimizar o impacto de incidentes;

f) Apoiar as áreas de desenvolvimento e de infraestrutura no controle de segurança da informação;

g) Promover o cumprimento dos objetivos estratégicos de TIC indicados no Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC 2018-2021;

h) Atingir conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais e com os demais padrões de segurança recomendados para órgãos da Administração Pública.

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

16.1. Não há 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. a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, na seguinte forma:

I - O(s) atestado(s) se aplicam aos itens 1, 3, 5, 7, 9, 11 e 14 do lote único (licenças perpétuas), os quais correspondem à parcela de maior relevância ou de valor significativo para o objeto deste certame.

II - O(s) atestado(s) deverão demonstrar o cumprimento de um quantitativo mínimo de 25% (vinte e cinco por cento) do volume estimado para cada um dos itens

acima referidos;

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 apresentadas pelas licitantes, desde que tais documentos sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

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

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

VI - 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 executados.

17.2. A motivação para a comprovação de aptidão técnica, bem como o percentual mínimo acima referido, se dá em virtude da realização do certame via Sistema de Registro de Preços com demanda em larga escala, para atendimento de 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

Será realizado teste de bancada na forma do previsto no Anexo IV deste documento.

19. OBRIGAÇÕES DO CONTRATANTE DE CONTRATADO

19.1. Obrigações da CONTRATANTE

19.1.1. São obrigações da CONTRATANTE:

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

19.2. Obrigações da CONTRATADA

19.2.1. 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:

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

b) Assinar o Termo de Confidencialidade e Sigilo, conforme o modelo a ser apresentado no futuro Termo de Referência

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

d) 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 definido neste documento, ficando resguardadas todas as demais obrigações constantes do futuro Edital.

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, pelas mesmas razões técnicas que inviabilizam o parcelamento do objeto.

20.2. Saliente-se que, no caso de o 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.

20.3. Também não se configura subcontratação o acordo de representação, revenda e uso de solução tecnológica de terceiros.

21. POSSIBILIDADE DE PARTICIPAÇÃO DE MICROEMPRESAS, PEQUENAS EMP0RESAS E EMPRESAS INDIVIDUAIS

21.1. É livre a participação de microempresas, empresas de pequeno porte e empresas individuais.

21.2. 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.

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

22. POSSIBILIDADE DE PARTICIPAÇÕES 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 e 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 do edital.

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.

22.1.5. 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 do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

22.2. **Possibilidade de participação de cooperativas**

22.2.1. Diante da especificidade desta contratação, que trata de serviços de solução tecnológica, envolvendo aquisição de licenças, com os respectivos serviços de manutenção, treinamento e de operação assistida e subscrição, 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 aplica a participação de cooperativas neste certame.

23. PRAZO DO CONTRATO E POSSIBILIDADES DE PRORROGAÇÃO

23.1. **Para os itens de compra (licenças perpétuas de software - itens 1, 3, 5, 7, 9, 11, 14).**

23.1.1. O prazo de vigência do contrato é de 180 (cento e oitenta) dias contados da data da divulgação no Portal Nacional de Contratações Públicas.

23.1.2. O prazo de vigência será automaticamente prorrogado, sem prejuízo da formalização adequada, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento e no Contrato.

23.1.3. O prazo contratual compreende o período previsto para o fornecimento e instalação, sem prejuízo dos prazos de garantia estabelecidos no contrato.

23.2. **Para o item de serviço sob demanda (treinamento - item 17).**

23.2.1. O prazo de vigência do contrato é de 12 (doze) meses, contados da data da sua

divulgação no Portal Nacional de Contratações Públicas.

23.2.2. O prazo de vigência será automaticamente prorrogado, sem prejuízo da formalização adequada, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento e no Contrato.

23.3. **Para os itens de serviço de natureza contínua (itens 2, 4, 6, 8, 10, 12, 13, 15, 16 e 18).**

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

23.3.2. 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.

23.3.3. **Quanto à instalação e configuração:**

23.4. Ficam valendo os prazos definidos nos subtópicos 25.2.1, I e III.

24. LOCAL DE ENTREGA DOS BENS/ PRESTAÇÃO DO SERVIÇO

24.1. Resguardada a forma de entrega informada no subtópico 25.1. deste documento, os atendimentos de suporte técnico e operação assistida, quando eventualmente necessários por meio presencial e envio de técnico ao local, serão realizados no endereço indicado pela Contratante.

24.2. 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 das licenças perpétuas (itens 1, 3, 5, 7, 9, 11 e 14, em parcela única, se dará de forma virtual, via e-mail cujo destinatário será informado na reunião de kick-off prevista neste documento.

25.1.2. A medição (entrega) dos serviços de manutenção e suporte técnico (itens 2, 4, 6, 8, 10, 12 e 15) será mensal, condicionada ao cumprimento do item 4.8.4.9, cuja dinâmica será informada na reunião de kick-off.

25.1.3. A entrega dos serviços de subscrição (itens 13 e 16), em parcela única, se dará de forma virtual, via e-mail cujo destinatário será informado na reunião de kick-off prevista neste documento.

25.1.4. A entrega dos serviços de treinamento (item 17), em parcelas sob demanda, acontecerá através do portal de treinamentos da CONTRATADA ou outro que esta venha a disponibilizar.

25.1.5. A entrega dos serviços de operação assistida (item 18), em parcelas sob demanda, ocorrerá de forma virtual, em modalidade remota, cuja dinâmica será informada na reunião de Kick-off. Entretanto, não obstante a entrega virtual, faz-se necessário o atendimento presencial para os casos de eventuais trocas de equipamentos ou componentes da solução.

25.2. **Prazo de Entrega**

25.2.1. Os cronogramas para as entregas do objeto, contados em dias úteis, ocorrerão conforme as tabelas abaixo:

25.2.2.

I - **Para os bens de compra (itens 1, 3, 5, 7, 9, 11 e 14):**

item	marco	Atividades	Prazo (dias corridos)	Responsável
1	Publicação do extrato do contrato	Realização da Reunião Kick-Off e emissão de Ordem de Fornecimento	05	CONTRATANTE e CONTRATADA
2	Emissão da Ordem de Fornecimento	Entrega das soluções (hardware+software+licença padrão) no ambiente do CONTRATANTE	05	CONTRATADA
3	Realização da reunião Kick Off	Instalação e configuração inicial completa da solução com a entrega do Relatório de Cumprimento do Objeto	20	CONTRATADA
4	Entrega do Relatório de Cumprimento do Objeto	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura	20	CONTRATANTE

II - Para os serviços de manutenção e suporte técnico (itens 2, 4, 6, 8, 10, 12 e 15), condicionados ao cumprimento do item 4.8.4.9:

item	marco	Atividades	Prazo (dias corridos)	Responsável
1	Emissão do Termo de Recebimento Definitivo relativo aos bens de compra (licenças perpétuas)	Emissão das Ordem de Início dos Serviços	05	CONTRATANTE
2	Emissão da Ordem de Início dos Serviços	Entrega do Relatório de Cumprimento do Objeto (mensal, condicionado ao cumprimento do item 4.8.4.9)	30	CONTRATADA
3	Entrega do Relatório de Cumprimento do Objeto	Emissão do Termo de Recebimento Provisório	02	CONTRATANTE
4	Emissão do Termo de Recebimento Provisório	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura	05	CONTRATANTE

III - Para os serviços de subscrição (itens 13 e 16 do lote único):

item	marco	Atividades	Prazo (dias corridos)	Responsável
1	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Realização da Reunião Kick-Off e emissão de Ordem de Serviço	05	CONTRATANTE e CONTRATADA
2	Realização da reunião Kick Off	Liberação do acesso à CONTRATANTE na plataforma SaaS da solução	03	CONTRATADA
3	Realização da reunião Kick Off	Início da implementação do escopo inicial de aplicações web que foram indicados pela CONTRATANTE na reunião de Kick-off	05	CONTRATADA
4	Realização da reunião Kick Off	Conclusão da implementação da configuração inicial básica da solução e Entrega do Relatório de Cumprimento do Objeto	20	CONTRATADA
5	Entrega do Relatório de Cumprimento do Objeto	Emissão do Termo de Recebimento Provisório	02	CONTRATANTE
6	Emissão do Termo de Recebimento Provisório	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura	05	CONTRATANTE

IV - Para os chamados abertos no âmbito dos serviços de manutenção se aplicam os prazos do Acordo de Nível de Serviço dispostos no subtópico 4.8.4.9 deste documento.

V - Para os serviços de treinamento (item 17 do lote único) as aulas deverão começar em até 20 dias úteis a contar da emissão da Ordem de Serviço, quando o CONTRATANTE não especificar prazos no documento. Os prazos para recebimento provisório e definitivo são os mesmos aplicados aos serviços de subscrição.

VI - Para os serviços de operação assistida (item 18 do lote único) os prazos de início e fim da realização das tarefas constarão na Ordem de Serviço. Os prazos para recebimento provisório e definitivo são os mesmos aplicados aos serviços de subscrição.

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

26.1. Os níveis dos serviços de suporte técnico, subscrições, operação assistida e treinamento, para fins de aferição de qualidade, observarão os critérios constantes no subtópico 4.11. e consideradas as glosas previstas no subtópico 4.12, ambos deste documento.

27. REGRAS PARA O RECEBIMENTO PROVISÓRIO E DEFINITIVO

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 os bens de aquisição (itens 1, 3, 5, 7, 9, 11 e 14) o recebimento das licenças ou aplicações será sumário, em até 2 (dois) dias úteis; e a instalação e configuração se dará conforme subtópico 25.2.1, I;

II - Para todos os serviços previstos, (itens 2, 4, 6, 8, 10, 12, 13, 15, 16, 17 e 18) 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;

III - A CONTRATADA deverá elaborar um Relatório de Cumprimento do Objeto (cujo modelo estará anexo ao futuro Termo de Referência) a ser entregue à Comissão de Fiscalização de Contrato quando da entrega provisória de quaisquer dos itens (bens e serviços). O relatório deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual. O relatório deverá estar acompanhado, conforme o bem ou serviço entregue, das seguintes informações e/ou documentos:

a) Para os bens de compra (itens 1, 3, 5, 7, 9, 11 e 14 do lote único): entrega das soluções adquiridas plenamente instaladas e configuradas; documentação que comprove o licenciamento desses bens, tais como: números de série ou credenciais ou chaves de acesso, dados para acionamento dos serviços de suporte e garantia, além dos documentos oficiais do fabricante e a documentação do produto (manuais, prospectos e quaisquer documentações pertinentes);

b) Para os serviços de manutenção, suporte técnico e de subscrição (itens 13 e 16 do lote único): documentação que comprove o licenciamento da solução contratada, tais como números de série ou credenciais ou chaves de acesso, bem como dados informativos para o acionamento do suporte técnico e documentos oficiais do fabricante e documentação do produto e a disponibilização da solução;

c) Para o serviço de treinamento (item 17 do lote único): certificados do(s) aluno(s) treinado(s);

d) Para o serviço de operação assistida (item 18 do lote único): os entregáveis previstos, conforme as respectivas tarefas demandadas, no catálogo de serviços previsto neste documento.

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 (bens e serviços) 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 o contrato ou termo de referência, podendo ser fixado pelo fiscal do contrato um prazo para a substituição do bem, ou o refazimento do serviço, às custas do contratado, sem prejuízo da aplicação das penalidades, sendo sempre necessário a motivação da recusa.

27.5. Estando 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:

a) 20 (vinte) dias corridos após o Recebimento Provisório e entrega do Relatório de Cumprimento do Objeto pela CONTRATADA, para os itens de compra;

b) 05 (cinco) dias úteis, depois do Termo de Recebimento Provisório e entrega do

Relatório de Cumprimento do Objeto, para os itens de subscrição, de treinamento e de operação assistida, serviços contínuos de manutenção.

27.7. Com o recebimento definitivo, que concretiza o ateste do cumprimento do objeto contratado, a CONTRATADA deverá emitir e enviar 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 excluem ou atenuam a responsabilidade da CONTRATADA, nem a exime de manter fiscalização própria.

28. CRITÉRIOS DE PAGAMENTO E FORMA DE REAJUSTAMENTO DO CONTRATO

28.1. **Forma e prazo de pagamento**

28.1.1. Pagamento conforme a natureza dos itens da seguinte forma:

I - Para os itens de compra (licenças perpétuas - itens 1, 3, 5, 7, 9, 11, 14)

a) A CONTRATANTE deverá pagar ao CONTRATADO em 1 (uma) parcela efetuada à vista.

II - Para os itens de serviços de Suporte/Manutenção (itens 2, 4, 6, 8, 10, 12, 15)

a) A CONTRATANTE deverá pagar ao CONTRATADO mensalmente, até o final da vigência do contrato.

III - Para os itens de serviços de Subscrição (licenças por anuidade - itens 13 e 16)

a) A CONTRATANTE deverá pagar o preço ao CONTRATADO em 1 (uma) parcela efetuada à vista.

IV - Para os itens de serviços de Treinamento e Operação Assistida (itens 17 e 18)

a) A CONTRATANTE deverá pagar o preço ao CONTRATADO, conforme a aferição da execução dos serviços.

28.2. **Reajuste de preços**

28.2.1. Para fins de reajuste dos preços contratados se faz razoável a aplicação pela CONTRATANTE, do Índice de Custos de Tecnologia da Informação – ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, de forma a resguardar o 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.

29. CONDIÇÕES DE GARANTIA CONTRATUAL

29.1. O Contrato contará com garantia de execução, nos moldes do art. 96 da Lei nº 14.133/2021, na forma abaixo explicitada:

29.1.1. 5% (cinco por cento) do valor total do contrato para os itens de compra (licenças perpétuas - itens 1, 3, 5, 7, 9, 11, 14);

29.1.2. 5% (cinco por cento) do valor inicial atualizado do contrato para o item de serviço por demanda (treinamento - item 17);

29.1.3. 5% (cinco por cento) do valor anual do contrato para os itens de serviços de natureza contínua (itens 2, 4, 6, 8, 10, 12, 13, 15, 16, e 18).

29.2. 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.

30. POSICIONAMENTO CONCLUSIVO

30.1. No presente estudo técnico e seus anexos estão apresentados os requisitos técnicos, legais, ambientais e os do próprio negócio, também os demais requisitos necessários para a caracterização e quantificação da demanda identificada, bem como foram demonstrados os aspectos do mercado em que o objeto se encontra inserido e o processo de escolha da solução que melhor se adequa às necessidades dos órgãos demandantes do presente estudo técnico, citados no subtópico 1.3.

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, a ser corroborada em pesquisa de preços, inclusive mediante consulta direta ao fornecedor, a ocorrer em fase posterior.

30.3. A contratação de solução de anonimização de dados e gerenciamento de chaves criptográficas é medida que, no caso concreto, se revela a opção mais vantajosa e mais condizente com o interesse público, resguardada a possibilidade de ampla competição de fornecedores.

30.4. Desta forma, entende-se ser VIÁVEL a contratação visando dar início à implementação do objeto, para o que 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 QUABNTO AO GRAU E PRAZO DE SIGILO

31.1. 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 registado 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 (119234905);

II - Mapa de Riscos (119234183);

III - Catálogo de Serviços (119233835);

IV - Teste de Bancada (119235090).

33. ASSINATURAS DOS MEMBROS DA EQUIPE RESPONSÁVEL PELO ESTUDO

Manuelito de Sousa Reis Junior Gerente de Riscos e Ameaças ID nº 4406953-7	**Vania Lucia Ventapane Soares** Técnica de Suporte ID nº 2823095-7	**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, na data da assinatura eletrônica.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 25/11/2025, às 15:25, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 25/11/2025, às 15:58, 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 25/11/2025, às 15:58, 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 **Vania Lucia Barros Ventapane Soares**, **Técnico de Suporte, Computação e Processamento**, em 25/11/2025, às 18:33, 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 **119421800** e o código CRC **9B805A06**.

Referência: Processo nº SEI-430002/001510/2024 SEI nº 119421800

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

ANEXO I ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

1.1. Características Básicas:

1.1.1. A solução ofertada deve reduzir ao máximo a ocorrência de incidentes internos de segurança, monitorando a atividade de usuários privilegiados (por exemplo: administradores, root, etc.), bem como possibilitar o impedimento do acesso a conteúdos de dados por estes usuários, sem que os mesmos percam privilégio administrativo no ambiente tecnológico.

1.1.2. A solução deve estabelecer o controle de acesso para o grupo de usuários mencionado no item 2.1.2, e deve também identificar atividades suspeitas, gerando logs destas mesmas atividades.

1.1.3. A solução deve estabelecer um modelo de proteção para informações de tal forma que o dado seja devidamente criptografado no sistema de arquivos. Desta forma, além de impedir a extração não autorizada, mesmo em caso de vazamento acidental dos dados, deverá garantir que os dados não possam ser acessados fora do ambiente gerenciado pela plataforma de segurança, pois neste caso não haveria a chave criptográfica necessária para acessar a informação.

1.1.4. A solução deve prover mecanismos de prevenção de infecção ou ataques a arquivos por malware, Ameaça Persistente Avançada (APT), ransomware, ataques através de acessos não-autorizados, modificações em bibliotecas entre outros, quando estes forem originados por usuários com acesso privilegiado.

1.1.5. A solução deve ser flexível e escalável, adequando-se às necessidades de crescimento da contratante.

1.1.6. A solução deve permitir a anonimização dos dados pessoais e/ou confidenciais, conforme definido no Art. 12 da Lei Geral de Proteção de Dados (LGPD).

1.1.7. A solução deve proteger sistemas de dados estruturados (banco de dados), bem como sistemas de dados não-estruturados (incluindo arquivos de aplicativos Microsoft, voz, vídeo e texto em geral) em um ambiente heterogêneo e de sistemas operacionais e plataformas de operação.

1.1.8. A solução deve suportar ao menos:

a) Sistemas operacionais: MS Windows Server, AIX e Linux;

b) Os bancos de dados suportados devem incluir: Oracle, MS-SQL, MySQL, Mongo DB, NoSQL, Teradata, SAP Hana e Hadoop Distributed arquivos. Desejável também: Maria DB, Postgres e Adabas;

c) Provedores de nuvem suportados devem incluir: AWS, S3, Azure, Office 365, SalesForce Shield, Rackspace, IBM Cloud e Google Cloud;

d) Todas as funcionalidades devem ser gerenciadas através do console de gerenciamento centralizado, a fim de facilitar o processo de administração, controle de acesso, gestão de logs e manutenção da solução de proteção de dados;

e) Soluções baseadas em software livre não serão aceitas.

1.1.9. O serviço deverá englobar as atividades relacionadas ao seu funcionamento, como manutenção evolutiva, preventiva e corretiva em software, sem quaisquer ônus adicionais para o contratante.

2. DESCRIÇÃO DOS ITENS

2.1. Console de Gerenciamento Centralizado em Alta Disponibilidade (Item 1):

2.1.1. A solução deverá prover uma console de gerenciamento composta por um conjunto integrado de produtos baseados em uma infraestrutura comum e extensível, com gerenciamento centralizado de políticas e de chaves, reduzindo o esforço de administração e o custo total de propriedade.

2.1.2. A console de gerenciamento deve oferecer recursos para proteger e controlar o acesso a bancos de dados, arquivos e contêineres. Deve também possibilitar a proteção de ativos que residam em nuvem, big data e ativos físicos e/ou virtuais.

2.1.3. A solução deve prover uma console única que permita o gerenciamento centralizado de todos os agentes de criptografia, suas chaves de criptografia, políticas de configuração, publicação e controle de acesso dos dados a serem protegidos.

2.1.4. A console deve atender aos padrões e requisitos da certificação FIPS 140-2, Common Criteria, ou outra equivalente, para garantir total segurança das chaves de criptografia.

2.1.5. A console de gerenciamento centralizado deve suportar agentes para as seguintes funcionalidades:

a) Criptografia transparente: para criptografar, controlar o acesso ao dado e oferecer registros de auditoria de acesso aos dados, sem impactar nas aplicações, bases de dados ou infraestrutura onde quer que os servidores estejam instalados;

b) Integração com SIEM: Suportar integração com os sistemas de gerenciamento de logs do mercado, como por exemplo Splunk, qRadar, Arcsight, McAfee, LogRhythm, etc;

c) Segurança de contêiner: Oferecer criptografia de dados, controle de acesso e registro de acesso ao dado;

d) Gerenciamento de chaves em nuvem múltipla: Permitir custódia e controle de dados em ambiente de software como serviço (SaaS), relatório de acesso e eficiência no gerenciamento do ciclo de vida da chave em nuvem com o conceito “Traga Sua Própria Chave - BIOK”;

e) Segurança de Big Data: Criar isolamento em seus data lakes, mascarar dados confidenciais e controlar a segurança e a conformidade de usuários e administradores;

f) Tokenização e mascaramento de dados: Reduzir os custos e o esforço necessários ao cumprimento das políticas de segurança e normas regulatórias como a LGPD, GDPR, PCI DSS, BACEN, dentre outras;

g) Criptografia para aplicações: Simplificar o processo de adição de criptografia em aplicações, por meio de API’s baseadas em padrões que potencializem operações criptográficas e de gerenciamento de chaves de alto desempenho.

2.1.6. A console deve ser capaz de ser configurada em alta disponibilidade (HA) com um servidor primário e outro secundário.

2.1.7. Apoiar a incorporação de vários consoles adicionais para fins de configuração de esquemas de tolerância a falhas multinível.

2.1.8. Os agentes instalados nos servidores devem operar de forma autônoma, de modo a não causar impacto em casos de perda de comunicação com a console.

2.1.9. Os agentes devem fazer a rotação/mudança de chaves sem indisponibilizar os servidores de dados.

2.1.10. Cada console deve ter a capacidade de suportar crescimento/escalabilidade.

2.1.11. Detalhes da chave criptográfica não devem ser divulgados para usuários do sistema, para que o algoritmo de criptografia esteja protegido dos usuários da plataforma. Estes devem ser armazenados de forma segura em dispositivo virtual dedicado aos serviços de segurança dentro da console.

2.1.12. A console deve possuir capacidade de gerenciar chaves criptográficas padrão KMIP.

2.1.13. Deve ser compatível com API PKCS#11 e Microsoft Key Extensible Management.

2.1.14. Deve ser capaz de oferecer suporte a certificados digitais (X. 509) PKCS#7, PKCS#8, PKCS#12, chaves de criptografia simétrica (algoritmos 3DES, AES128, AES256, ARIA128, ARIA256) e também assimétrica (algoritmos RSA1024, RSA2048, RSA4096).

2.1.15. A solução deve ser escalável para oferecer suporte ao gerenciamento de agentes de vários serviços em uma estrutura de multi-tenant e com suporte a configuração de segurança de vários domínios. Para isso, deve possibilitar configurar diferentes chaves criptográficas de acordo com cada área de operação, se necessário.

2.1.16. Quando aplicada a separação de funções, a console deve permitir que o usuário do sistema crie chaves de criptografia, outro usuário pode aplicá-las e outro, que não seja o anterior, consiga monitorar o mesmo durante a aplicação.

2.1.17. A console deve possibilitar o gerenciamento, via interface web, a utilização de comando (CLI) e API (REST).

2.1.18. A solução deve possibilitar requerer autenticação de usuário e senha e, opcionalmente, dois fatores RSA.

2.1.19. Deve ser capaz de configurar cópias de backup de suas configurações automaticamente ou manualmente.

2.1.20. Requerimentos complementares:

I - Suportar usuários múltiplos;

II - Cluster para alta disponibilidade (HA);

III - Toolkit e interface de programação;

IV - Integração com infraestrutura de autenticação existente, com fácil configuração;

V - Suporte para API RESTfull;

VI - Opções de instalação:

a) Sistema virtual com padrões e requisitos da certificação FIPS 140-2 Nível, ou certificação compatível;

b) O sistema virtual deve ser compatível com VMware, Hyper-V, KVM, AWS e Azure;

c) Sistema de hardware com padrões e requisitos de certificação FIPS 140-2 Nível 2, ou compatível;

d) Sistema de hardware com padrões e requisitos da certificação FIPS 140-2 Nível 3, ou compatível.

2.2. **Agentes de Proteção de Dados para Bancos de Dados (Item 3):**

2.2.1. Este agente deve fornecer criptografia de banco de dados (dados estruturados) para dados em repouso com gerenciamento centralizado de chaves, controle de acesso de usuários, incluindo usuários privilegiados, e registro detalhado de auditoria de acesso, visando atender aos requisitos de conformidade e práticas recomendadas para proteger os dados, onde quer que estejam. O agente deverá residir no sistema operacional ou na camada de dispositivo, a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela;

2.2.2. O processo de criptografia deve ser executado por agentes que serão instalados nos servidores de banco de dados;

2.2.3. Esses agentes devem oferecer suporte a sistemas operacionais MS Windows Server, AIX e Linux;

2.2.4. Eles devem ser compatíveis com bancos de dados estruturados e não-estruturados, incluindo MS-SQL Server, Oracle, NoSQL, MySQL, MongoDB e sistema de arquivos distribuídos Hadoop;

2.2.5. Deve ser compatível com servidores físicos e versões virtualizadas;

2.2.6. Sua implementação não deve exigir qualquer alteração no banco de dados ou na aplicação;

2.2.7. Estes devem usar os recursos de aceleração disponíveis, como o AES-NI. A implementação destes não deve gerar uma carga incremetal, típica em servidores, maior que 5%;

2.2.8. Além de criptografar o banco de dados, os agentes devem ser capazes de criptografar arquivo, volume ou diretório desses servidores de forma que eles possam proteger informações estruturadas e não-estruturadas (exemplo: imagens, vídeo, arquivos de áudio, syslog, etc.);

2.2.9. Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso;

2.2.10. As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema, e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio;

2.2.11. Deve ser possível basear tais diretivas em: usuário, processo, tipo de arquivo e agendamento;

2.2.12. As políticas devem poder ser aplicadas aos usuários locais, ou integradas no AD ou LDAP;

2.2.13. Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com a console de gerenciamento para poder aplicar processos de criptografia e descriptografia;

2.2.14. A solução deve possibilitar o envio de logs de atividades para uma solução de SIEM através de um servidor de syslog, ou no formato CEF, em tempo real e nativamente;

2.2.15. A solução deve suportar ao menos os seguintes ambiente em nuvem: AWS, Azure, Rackspace e IBM;

2.2.16. A solução deve ter capacidade de integrar os serviços de gerenciamento de chaves, fornecendo serviços de gerenciamento de chaves on premisse ou em nuvem;

2.2.17. A solução deve registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos;

2.2.18. A solução deve possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados;

2.2.19. Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não-criptografado;

2.2.20. Requerimentos complementares:

a) Compatibilidade com os sistemas operacionais: Windows Server 2016, 2019 R2 (64 bits) e superiores; Red Hat e CentOS 7.5-8.0e superiores, SLES 12 SP4, SLES 12 SP5, SLES 15 e superiores, Ubuntu 16, 18, 20 e superiores; Oracle Linux (versão corrente).

2.3. **Agentes para Compartilhamento Seguro de Bases de Dados (Item 5):**

2.3.1. Este agente deve permitir o mascaramento dos dados sensíveis para permitir o compartilhamento seguro com terceiros, ambientes de teste, ambientes de desenvolvimento e outros casos de uso aplicáveis;

2.3.2. O funcionamento deve ser baseado em tabela e/ou coluna. Informa-se o que deverá ser mascarado no novo banco de dados de destino. Desta forma, dados não identificados podem ser compartilhados;

2.3.3. A solução deve ser customizável e de alta performance;

2.3.4. A solução deve suportar ao menos as operações de criptografia / tokenização e descriptografia / de-tokenização de tabelas e/ou colunas;

2.3.5. A solução deve ser transparente para a aplicação ou banco de dados com acesso via conexão ODBC. Ou seja, não deve requerer alterações ou instalações adicionais no servidor de banco de dados;

2.3.6. A solução deve suportar, ao menos, arquivo CSV, Oracle, Microsoft SQL Server, MySQL e DB2;

2.3.7. A solução deve permitir replicação de arquivo para arquivo, banco de dados para banco de dados, arquivo para banco de dados e banco de dados para arquivo;

2.3.8. Pelo menos os seguintes modelos devem ser suportados: Standard AES Encryption, Batch random Tokenization e Batch FPE FF3/FF1.

2.4. **Agentes de Proteção de Dados para Servidores de Arquivos - File Server (Item 7):**

2.4.1. Este agente deve fornecer criptografia de servidor de arquivo (dado não estruturado) para dados em repouso com gerenciamento centralizado de chaves, controle de acesso de usuários, incluindo usuários privilegiados, e registro detalhado de auditoria de acesso, visando atender aos requisitos de conformidade e práticas recomendadas para proteger os dados, onde quer que estejam. O agente deverá residir no sistema operacional ou na camada de dispositivo, e a criptografia e a descriptografia devem ser transparentes para todos os aplicativos executados acima dela;

2.4.2. O processo de criptografia deve ser executado por agentes que deverão ser instalados nos servidores de arquivos;

2.4.3. Os agentes devem ser compatíveis com sistemas operacionais Microsoft e Linux;

2.4.4. Deve ser compatível com servidores físicos e virtuais;

2.4.5. Sua implementação não deve exigir qualquer tipo de alteração no servidor de arquivo ou processo para manuseio do dado pelo usuário final;

2.4.6. Deve ser capaz de criptografar o arquivo, volume ou diretório desses servidores, de forma que eles possam proteger informações não estruturadas (por exemplo: imagens, vídeos, arquivos de voz, syslog, etc.);

2.4.7. Os agentes devem registrar e rastrear o acesso dos usuários de sistema aos arquivos, e ser capaz de bloquear ou restringir este acesso;

2.4.8. As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema, e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio;

2.4.9. A solução deve permitir que as diretivas possam ser baseadas em usuário, processo, tipo de arquivo;

2.4.10. As políticas devem ser aplicadas aos usuários locais, ou igualmente integradas no AD ou

2.4.11. LDAP;

2.4.12. Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com a console de gerenciamento para que possam ser aplicados processos de criptografia e descriptografia;

2.4.13. Os logs de atividade do usuário devem ter a capacidade de serem enviados para uma solução de SIEM através de um servidor de syslog ou no formato CEF, em tempo real e nativamente;

2.4.14. A solução deve suportar ao menos os seguintes ambientes em nuvem: AWS, Azure, Rackspace, IBM e Compute Engine (Google);

2.4.15. Deve registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos;

2.4.16. Deve possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados;

2.4.17. Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não-criptografado;

2.4.18. Requerimentos complementares:

a) Compatibilidade com os sistemas operacionais: Windows Server 2016, 2019 R2 (64 bits) e superiores; Red Hat e CentOS 7.5-8.0e superiores, SLES 12 SP4, SLES 12 SP5, SLES 15 e superiores, Ubuntu 16, 18, 20 e superiores; Oracle Linux (versão corrente).

2.5. **Agentes de Proteção de Dados para Contêineres (Item 9):**

2.5.1. Este agente deve prover criptografia, controle de acesso e registro de acesso à dados para estabelecer segurança em torno dos ambientes dinâmicos dos contêineres. Com este agente, a criptografia, os controles de acesso e o registro de auditoria de acesso podem ser aplicados em cada contêiner, tanto para dados dentro de contêineres quanto para armazenamento externo acessível a partir de contêineres;

2.5.2. O processo de criptografia deve ser executado por agentes que serão instalados nos contêineres;

2.5.3. Sua implementação não deve exigir qualquer alteração no contêiner ou processo para manuseio do dado pelo usuário final;

2.5.4. Deve ser capaz de criptografar arquivo, volume ou diretório, assim protegendo os dados;

2.5.5. Os agentes devem registrar e rastrear o acesso dos usuários e ser capaz de bloquear ou restringir este acesso;

2.5.6. As políticas de controle de acesso devem poder ser aplicadas mesmo aos usuários privilegiados do sistema, e estes não devem possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio;

2.5.7. Tais diretivas devem permitir terem como base: usuário, processo, tipo de arquivo e agendamento;

2.5.8. As políticas devem poder ser aplicadas aos usuários locais, ou igualmente integradas no AD ou LDAP;

2.5.9. Os agentes devem ter a capacidade de armazenar chaves de criptografia em memória para que eles não exijam conectividade com a console de gerenciamento para poder aplicar processos de criptografia e descriptografia;

2.5.10. Os logs de atividade do usuário devem poder ser enviados para uma solução de SIEM através de um servidor de syslog, ou no formato CEF, em tempo real e nativamente;

2.5.11. Registrar todas as tentativas de acesso permitido, negado e restrito de usuários, aplicativos e processos;

2.5.12. Possuir políticas de acesso baseadas em função para controlar quem, o que, onde, quando e como os dados podem ser acessados;

2.5.13. Permitir que usuários privilegiados executem seu trabalho sem acesso a dados em texto não-criptografado;

2.5.14. Requerimentos complementares:

a) Compatibilidade com as plataformas: Docker, Red Hat OpenShift, RHEL 7.x, executar em servidores físicos, VM’s e instâncias AWS EC2.

2.6. **Agentes de Proteção de Dados para Aplicação (item 11):**

2.6.1. Este agente deve permitir a tokenização vaultless com o Dynamic Data Masking, para anonimizar dados de maneira eficiente, incluindo dados pessoais, quer eles residam on premise, ambientes de big data ou em nuvem. Com isso, reduzir o escopo de conformidade substituindo dados confidenciais por um token não-sensível que olha e age como o original, ou seja, proteção de dados sem a necessidade de alterar bancos de dados. Após a substituição dos dados pelo token, os sistemas não estão mais sujeitos a conformidade, significando menor esforço para atender regulamentações;

2.6.2. Possuir alto desempenho com baixo impacto na performance da aplicação;

2.6.3. Possuir servidores de token virtual escalável;

2.6.4. Comunicação via TLS autenticando mutuamente;

2.6.5. Interface REST API com chamadas individuais e em lote;

2.6.6. Permitir geração de tokens aleatórios;

2.6.7. Compatibilidade com FPE FF1, tokens FF3;

2.6.8. Permitir mascaramento dinâmico ou estático de dados;

2.6.9. Gerenciamento de chaves e políticas

2.6.10. Suporte AD / LDAP;

2.6.11. Suporte a dados numéricos e alfanuméricos;

2.6.12. Permitir a criação de tokens em formato numérico, de texto e de data, para aplicativos únicos ou múltiplos;

2.6.13. Permitir utilizar grupos de usuários LDAP para decidir quais informações são exibidas para grupos específicos. Por exemplo, operadores de call center versus gerentes de call center;

2.6.14. Suportar servidor de tokens em formato virtual, como por exemplo: OVF, ISO, Microsoft Azure, MarketPlace ou Amazon AMI;

2.6.15. Restringir o acesso a ativos confidenciais sem alterar os esquemas do banco de dados, sem interrupções;

2.6.16. Proteger dados em trânsito e em repouso;

2.6.17. Mascarar os dados em ambiente de desenvolvimento, teste e terceirizados com acesso ao banco de dados;

2.6.18. Proteger DBA's, administradores de sistema, root, de usuários mal-intencionados com acesso direto ao banco, uma vez que os dados que estes irão acessar, não serão os dados reais;

2.7. **Subscrição de Agentes para Gestão de Chaves na Nuvem – Termo de Licenciamento por 12 meses (Item 13):**

2.7.1. Este agente deve prover o controle de chave pelo próprio cliente permitindo a separação, criação, propriedade, controle e revogação das chaves de criptografia sem a dependência do provedor. Deverá reduzir a complexidade do gerenciamento de chaves, dando ao próprio cliente controle de ciclo de vida de chaves de criptografia com gerenciamento centralizado, visibilidade e rastreabilidade;

2.7.2. Deverá cumprir com os regulamentos de proteção de dados e armazenamento de chaves rigorosos podendo chegar aos padrões e requisitos da certificação FIPS 140-2 Nível 3, ou certificação

2.7.3. equivalente;

2.7.4. Prover eficiência com gerenciamento de chave centralizado em ambientes de nuvem híbrida;

2.7.5. Fornecer acesso a cada provedor de nuvem a partir de uma única janela do navegador, incluindo várias contas ou assinaturas;

2.7.6. Rotacionar de forma automática as chaves para cumprir com regulamentações que exigem este serviço de rotação de chave;

2.7.7. Fornecer mecanismos simples, via login federado, para conceder acesso aos dados. Com isso, ser compatível com logins de serviços em nuvem que são autenticados e autorizados pelo provedor de serviços, isto é, nenhum banco de dados de login nem configuração AD ou LDAP é necessário;

2.7.8. Fornecer meios para solicitar a criação de chaves nos provedores de nuvem e fornecer gerenciamento completo do ciclo de vida das mesmas;

2.7.9. Controlar e gerenciar centralizadamente várias nuvens, IaaS e SaaS (Multicloud);

2.7.10. Prover registro (log), rastreabilidade e relatórios de conformidade totalmente independente do provedor de nuvem;

2.7.11. O agente deve suportar, pelo menos, os provedores de nuvem que seguem: Microsoft Azure, Microsoft Office365, Microsoft Azure Stack, Amazon Web Services, Salesforce.com e Compute Engine (Google);

2.7.12. A subscrição dos "Agentes para Gestão de Chaves na Nuvem" abrangerá também o suporte técnico e atualização de versão em moldes semelhantes aos dos serviços de itens 2, 4, 6, 8, 10, 12 e 15 do lote único do objeto.

2.7.13. O período de subscrição dos Agentes para Gestão de Chaves em Nuvem será de 12 (doze) meses.

2.8. **Agentes para Gestão de Chave Local (Item 14):**

2.8.1. Ser capaz de centralizar o gerenciamento de chaves de aplicativos de terceiros que usam criptografia nativa, tal como bancos de dados;

2.8.2. O agente deve ter a capacidade de conectar-se com os aplicativos por meio de interfaces padrão e fornecer acesso às funções robustas de gerenciamento de chaves;

2.8.3. Prover simplificação e redução da carga operacional por meio do gerenciamento centralizado de chaves;

2.8.4. Elevar o nível de segurança pela separação das chaves de criptografia das aplicações, banco de dados, storage e etc;

2.8.5. Gerenciar chave utilizando soluções de hardware ou software com padrões e requisitos da certificação FIPS ou equivalente;

2.8.6. Suportar o protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP / PKCS) que é o padrão do setor para troca de chaves de criptografia entre clientes (usuários principais) e um servidor (armazenamento de chaves). A padronização simplifica o gerenciamento de chaves externas;

2.8.7. Garantir a custódia de chaves para, pelo menos: Oracle TDE, SQL TDE, Nutanix, VMWare, Cisco, Netapp, Certificados, Aplicações desenvolvidas em casa, outros volumes compatíveis;

2.9. **Subscrição de Agentes para Descoberta e Classificação de Dados (Item 16):**

2.9.1. A solução deverá possibilitar a descoberta de dados, em ambiente de dados estruturados e não estruturados, armazenados em diferentes repositórios, tais como: Servidores de Arquivos; Bancos de Dados; Big Data; Estações de trabalho;

2.9.2. A funcionalidade de descoberta de dados deverá ser fornecida na modalidade subscrição de

2.9.3. serviço, onde o contratante pagará mensalmente tendo por base o quantitativo de dados efetivamente tratados (em terabytes);

2.9.4. A solução deve permitir, através de interface única, realizar o levantamento e entendimento dos dados existentes, sua localização e riscos associados, permitindo: Atender aos requisitos de privacidade; obter visibilidade sobre os dados que estão em risco de exposição; suportar a criação de plano de privacidade e proteção de dados;

2.9.5. A solução ofertada deverá possibilitar, pelo menos, quatro níveis de classificação de dados por padrão: Restrito; Privado; Interno; Público;

2.9.6. A solução deve atribuir pontuações de risco que permitam identificar o nível de sensibilidade dos dados, como arquivos e bancos de dados, agregando os seguintes parâmetros: nível de proteção; quantidade de elementos encontrados; localização; quantidade de dados confidenciais;

2.9.7. As pontuações de risco devem permitir identificar os dados com maior exposição e permitir priorizar medidas de proteção;

2.9.8. A solução deve suportar os seguintes ambientes: Armazenamento local em Hard Disk e Memória dos computadores; Armazenamentos em rede: Compartilhamento Windows CIS e SMB; Unix File System NFS; Bancos de Dados: IBM DB2; Oracle; SQL; Big Data: Clusters Hadoop. Desejável também: Maria DB, Postgres e Adabas;

2.9.9. A solução deve suportar os seguintes tipos de arquivos:

a) Banco de Dados: Access; Dbase; SQLite; MSSQL MDF & LDF;

b) Arquivos de Imagens: BMP; FAX; GIF; JPG; PDF; PNG; TIF

c) Arquivos Compactados: bzip2; Gzip (todos os tipos); TAR; Zip (todos os tipos);

d) Microsoft Backup: Microsoft Binary / BKF;

e) Microsoft Office : v5, 6, 95, 97, 2000, XP, 2003 e superiores;

f) Open Source: Star Office; Open Office e LibreOffice;

g) Padrões abertos: PDF; HTML; CSV; TXT.

2.9.10. A solução deve classificar os dados como: dado pessoal; dados financeiros, com base em modelos integrados ou técnicas de classificação;

2.9.11. Deve possibilitar a identificação de informações padronizadas do Brasil, tais como: Registro Geral (RG); CPF; CNH; Passaporte;

2.9.12. A solução deve permitir a inclusão de modelos de políticas (descoberta e classificação) específicas para LGPD;

2.9.13. A solução deve fornecer relatórios detalhados para demonstrar conformidade com a Lei Geral de Proteção de Dados (LGPD);

2.9.14. A solução deve possibilitar a classificação de dados utilizando: regex, Patterns, algoritmos, contexto;

2.9.15. A solução deve permitir ser implementada “com” ou “sem” agentes instalados;

2.9.16. A solução deve possuir as seguintes características funcionais:

a) Políticas: definir as políticas de privacidade de dados, locais e perfis de varredura e de classificação;

b) Descoberta: localizar dados estruturados e não estruturados, através de toda a organização em ambientes big data, banco de dados e sistema de armazenamento de arquivos;

c) Classificação: classificar dados pessoais e sensíveis, baseado em modelos pré-configurados e técnicas de classificação;

d) Análise de risco: entender a natureza do dado e seus riscos, oferecendo visualizações;

e) Relatórios: gráficos e relatórios de análise de risco, status e alertas durante todo o ciclo de vida do dado;

A subscrição dos “Agentes para Descoberta e Classificação de Dados” abrangerá também o suporte técnico e atualização de versão em moldes semelhantes aos dos serviços de itens 2, 4, 6, 8, 10, 12 e 15 do lote único do objeto.

2.10. **Serviços de Manutenção, Suporte Técnico e Atualização de Versão para Solução de Gerenciamento de Chaves Criptográficas (itens 2, 4, 6, 8, 10, 12 e 15):**

2.10.1. As seguintes especificações de suporte irão vigorar para todos os itens de “**serviços de manutenção, Suporte Técnico e atualização de versão**” ofertados na ARP, correspondendo aos Itens 2, 4, 6, 8, 10, 12 e 15 do lote único.

2.10.2. Os "serviços de manutenção, suporte técnico e atualização de versão" terão duração de 12 (doze meses), prorrogáveis por iguais períodos até o limite estabelecido pela Lei Federal 8.666;

2.10.3. O pagamento dos “serviços de manutenção, suporte técnico e atualização de versão” será realizado mensalmente, e seu início, inclusive para fins de pagamento, ocorrerá após a instalação completa da Solução, na forma do cronograma do Estudo Técnico Preliminar;

2.10.4. 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);

2.10.5. Os "serviços de manutenção, suporte técnico e atualização de versão" contarão também com atendimento telefônico, exclusivamente em língua portuguesa (PT-BR), e disponível no regime 24x7;

2.10.6. A contratante poderá efetuar um número ilimitado de chamados para suporte técnico (on-line e on-site), sem custo adicional ao Contratante, durante a vigência do contrato, para suprir suas necessidades com relação aos serviços contratados. O suporte on-line deverá disponibilizar ferramenta de

acesso remoto e proporcionar o referido acesso quando solicitad, mediante autorização do Contratante;

2.10.7. Entende-se por manutenção todos os procedimentos destinados ao reestabelecimento operacional da solução com todas as suas funcionalidades, motivados pela ocorrência de incidentes na solução e/ou problemas recorrentes na solução, ajustes, reparos e correções necessárias.

2.10.8. A manutenção será destinada a remover os defeitos apresentados pelos componentes de software de todo o objeto do contrato, compreendendo também a atualização de versões que se fizerem necessárias;

2.10.9. A manutenção será realizada sempre que a solução apresentar falha que impeça o seu funcionamento regular e requeira uma intervenção técnica especializada e mesmo a substituição de seus componentes;

2.10.10. Durante a manutenção, a contratada deverá analisar a solução, sua atual condição de funcionamento, seus logs de sistema e sugerir mudanças para uma melhor prática de utilização da ferramenta. A equipe técnica do contratante decidirá sobre a aplicação ou não das recomendações;

2.10.11. Cada pessoa cadastrada no sistema como usuário deverá receber identificação e senha que permitam acesso seguro tanto ao sistema, como ao recurso de abertura de chamadas de suporte técnico, de maneira a evitar que pessoas não autorizadas possam acionar o serviço;

2.10.12. Também farão parte do escopo do “serviços de manutenção, suporte técnico e atualização de versão”:

a) Troubleshooting problemas de comunicação com os agentes;

b) Escalação de problemas para as áreas responsáveis de Administração e Operação;

c) Atuação em chamados de problemas e incidentes abertos no Help Desk;

d) Atualização dos chamados;

e) Apoio e esclarecimento de causa raiz do problema;

f) Detalhamento da solução adotada;

g) Documentação de evidências;

h) Correções de falhas (bugs) de software;

i) Realizar substituição de equipamentos ou componentes de hardware que componham a solução, caso necessário;

j) Executar as demais atualizações de software necessárias ao bom funcionamento da solução.

2.10.13. Para efeito de avaliação dos níveis de serviços prestados nos "serviços de manutenção, suporte técnico e atualização de versão", considerar-se-á a contagem do tempo de atendimento a partir da abertura do chamado, independentemente desta ter sido realizada fora do horário comercial;

2.10.14. Devem ser cumpridos os prazos máximos para resposta aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme abaixo:

Classificação	**Descrição**	**Prazo para iniciar o Atendimento (em horas)**	**Tempo máximo de Solução (em horas)**
Urgente	Problema técnico que impeça a utilização da solução em sua totalidade.	1	2
Alta	Problema técnico que impeça completamente a utilização de uma funcionalidade.	1	8
Média	Problema técnico que impeça a utilização parcial de uma funcionalidade, não impedindo por completo seu uso.	2	24

Baixa	Problema técnico que gere pouco ou baixo impacto na utilização da solução.	4	48
Informação	Consulta técnica, dúvidas em geral, monitoramento	4	48

2.10.15. Para fins de atestação de fatura, a contratada deverá fornecer mensalmente, relatórios sobre a prestação dos serviços, preferencialmente em formato PDF, constando as seguintes informações:

a) informações analíticas e sintéticas sobre os serviços realizados, incluindo-se chamados abertos e fechados, enfatizando aqueles resolvidos no período.

b) todos os chamados ocorridos no período, data e hora de abertura do chamado, data e hora de início do atendimento, data e hora de fechamento do chamado, nome da pessoa que abriu o chamado, nome da pessoa que efetuou o atendimento, descrição do problema e descrição da solução.

c) dados da reabertura de chamados, quando for o caso, que foram fechados sem serem devidamente resolvidos e que, por esse motivo, necessitaram ser reabertos;

d) cada solicitação de suporte remoto, contendo data e hora da solicitação de suporte técnico, do início e do término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes.

2.11. **Serviço de Treinamento para Solução de Anonimização (tem 17)**

2.11.1. O treinamento de capacitação técnica será ministrado por aluno, selecionado pela contratante, com carga horária mínima de 40 (quarenta) horas, material oficial do fabricante, e conteúdo necessários a capacitá-los para utilizar o Sistema ofertado;

2.11.2. Deverá ser emitido certificado de participação ao final do curso;

2.11.3. Todo o material didático deve ser repassado de forma impressa e em mídia para os alunos;

2.11.4. Somente serão aceitos materiais oficiais dos fornecedores do Sistema ofertado, e não será permitida a adaptação sobre apostilas/conteúdos de cursos não oficiais;

2.11.5. Os instrutores deverão possuir certificação comprovada nas soluções ofertadas;:

2.11.6. O treinamento deverá ocorrer nas dependências da CONTRATANTE, ou ainda remotamente, em ambiente virtual, ficando a contratada responsável por montar o ambiente adequado para realização do mesmo, isto é, todo o espaço necessário assim como toda infraestrutura computacional e de rede necessária. Caberá à CONTRATADA instalar a Plataforma de anonimização e gerenciamento de chaves criptográficas ou possibilitar o acesso ao Sistema no ambiente de treinamento;

2.11.7. Todas as despesas relativas à execução do treinamento serão de exclusiva responsabilidade da CONTRATADA, incluindo os gastos com instrutores, seu deslocamento e hospedagem, a confecção e distribuição dos originais do material didático e a emissão de certificados para os profissionais treinados;

2.11.8. O treinamento deverá iniciar em até 30 dias a contar da emissão da Ordem de Serviço.

2.12. **Serviço Técnico Especializado (tem 18)**

2.12.1. O serviço técnico especializado encontra-se detalhado no Anexo III do Estudo Técnico Preliminar.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 25/11/2025, às 15:58, 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 25/11/2025, às 15:58, 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 **Vania Lucia Barros Ventapane Soares**, **Técnico de Suporte, Computação e Processamento**, em 25/11/2025, às 18:33, 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 **119234905** e o código CRC **5EDF5124**.

Referência: Processo nº SEI-430002/001510/2024 SEI nº 119234905

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. Contratação de empresa para o fornecimento e prestação de serviços de solução para gerenciamento de chaves criptográficas incluindo os serviços de instalação, configuração, integração, manutenção, suporte técnico, operação assistida e treinamento da solução, na forma estabelecida do Estudo Técnico Preliminar.

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

3.1. 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 Referencia.	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

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 25/11/2025, às 15:25, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 25/11/2025, às 15:58, 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 25/11/2025, às 15:58, 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 **Vania Lucia Barros Ventapane Soares**, **Técnico de Suporte, Computação e Processamento**, em 25/11/2025, às 18:33, 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 **119234183** e o código CRC **D401CF36**.

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

ANEXO - III CATÁLOGO DE SERVIÇOS

1. CATÁLOGO DE SERVIÇOS REFERENTES À UNIDADE DE SERVIÇOS TÉCNICOS - UST

1.1. O catálogo de serviços estabelece as atividades dentro de cada fase da operacionalização da plataforma de gestão de chaves criptográficas com a complexidade de execução de cada item. As Ordens de Serviço para execução dos projetos serão realizadas a partir do consumo de UST dos itens do catálogo.

1.2. Os serviços técnicos especializados relativos aos sistemas e suporte a soluções de automação com atendimento remoto e on-site (no local), serão realizados sob demanda, a partir de um conjunto de atividades estabelecido no Catálogo de Serviços, aqui apresentado, em consonância com as etapas previstas no planejamento de execução dos projetos, e estabelece uma sequência de atividades que podem ser aplicadas no desenvolvimento de cada projeto, bem como, da complexidade típica esperada na realização das atividades preconizadas.

1.3. Os serviços técnicos especializados terão como unidade de medida a "unidade de serviço técnico" (UST) e serão requisitados, sob demanda, por meio de ordem de serviço.

1.4. O modelo de quantificação por UST é baseado na quantificação detalhada de cada esforço de trabalho realizado para obtenção dos serviços necessários no escopo deste Estudo Técnico Preliminar.

1.5. A fim de uniformizar o entendimento sobre os termos utilizados, seguem algumas definições:

- Unidade de Serviço Técnico – UST: métrica utilizada para aferir o custo de cada atividade a ser desempenhada;
- Custo em UST – representa o custo de cada atividade, considerando o tempo de duração em UST e o peso de cada UST; e
- Duração em UST – Tempo de duração para execução de cada atividade, considerando que uma UST tem a duração de 60 minutos.

1.6. A tabela a seguir apresenta o quantitativo de UST para cada hora de trabalho dados os respectivos graus de complexidade:

COMPLEXIDADE	FATOR DE PONDERAÇÃO
Baixa	**1**
Média	**2**
Alta	**3**

1.7. De acordo com a elevação do nível de complexidade da atividade especificada, é necessário o aumento da especialização do profissional, que dará cumprimento a cada rotina da demanda e o ajuste proporcional da UST.

1.8. Tabela de Quantidades Consolidadas por Fase, conforme o Catálogo de Serviços listado abaixo:

	Catálogo de Serviços Por Demanda										
Item	**Atividade**	**Descritivo**	**Perfil Profssional**	**Produto**	**Considerações**	**Métrica**	**UST's Estimadas (por serviço)**	**Complexidade**	**QTD. de Serviços**	**Fator de Ponderação**	**UST's Estimadas**
1	**Projeto Executivo**	**Levantamento de recomendações, riscos, premissas e restrições;**	**Gerente de Projeto**	**Projeto executivo (documento) consolidando as informações contempladas.**	**Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para elaboração de projeto executivo com vistas a operacionalizar a solução por completo, alinhada com os objetivos da contratação. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é de uma unidade por solução adquirida. O serviço poderá ser demandado após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.**	**Uma unidade de atividade por solução adquirida.**	**5**	**Alta**	**1**	**3**	**15**
		Definição da equipe envolvida e respectivas funções de cada indivíduo;	**Gerente de Projeto**				**2**	**Alta**	**1**	**3**	**6**
		Elaboração de Plano de Comunicação operacional;	**Gerente de Projeto**				**5**	**Alta**	**1**	**3**	**15**
		Elaboração de matriz de responsabilidades;	**Gerente de Projeto**				**2**	**Alta**	**1**	**3**	**6**
		Mapeamento de objetivos a serem alcançados;	**Gerente de Projeto**				**5**	**Alta**	**1**	**3**	**15**
		Definição de atividades, prazos e responsáveis que serão realizadas ao longo do contrato.	**Gerente de Projeto**				**16**	**Alta**	**1**	**3**	**48**
		Definição de cronograma macro, abrangendo toda a vigência do contrato, detalhando atividades, prazos e responsáveis definidos;	**Gerente de Projeto**				**15**	**Alta**	**1**	**3**	**45**
		Definição de reuniões sazonais para ponto de controle entre as partes, a fim de avaliar, monitorar e ajustar o andamento das atividades previstas.	**Gerente de Projeto**				**4**	**Alta**	**1**	**3**	**12**

2	Parametrização da Console de Gerenciamento Centralizado	Implementação e validação da operação em alta disponibilidade;	Especialista Componente	Relatório com evidências de todas as parametrizações executadas	Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para parametrização da console de gerenciamento centralizado de chaves criptográficas. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é de uma unidade por solução adquirida. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.	Uma unidade de atividade por solução adquirida.	15	Alta	1	3	45
		Definição e implementação de estratégia de perfis e funções de usuários;	Especialista Componente				8	Alta	1	3	24
		Criação de usuários;	Especialista Componente				2	Alta	1	3	6
		Integração com SIEM, caso a CONTRATANTE possua;	Especialista Componente				3	Alta	1	3	9
		Definição do rotacionamento de chaves criptográficas;	Especialista Componente				2	Alta	1	3	6
		Parametrização de alertas e notificações	Especialista Componente				2	Alta	1	3	6
3	Parametrização de Agentes	Integração do agente com a console de gerenciamento centralizado;	Analista de Segurança Pleno	Relatório com evidências das parametrizações executadas	Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para parametrização de agentes. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é igual ao somatório de todos os agentes que compõem a aquisição. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.	A quantidade de execuções desta atividade ao longo da vigência é igual ao somatório de todos os agentes que compõem a aquisição (ex. 5 agentes).	2	Média	5	2	20
		Definição de usuários e perfis, de acordo com o respectivo agente.	Analista de Segurança Pleno				2	Média	5	2	20
		Integração e comunicação com os ativos alvos de proteção, de acordo com o respectivo agente	Analista de Segurança Pleno				5	Média	5	2	50
		Definição e implementação de rotinas operacionais, de acordo com o respectivo agente;	Analista de Segurança Pleno				5	Média	5	2	50
		Definição do rotacionamento de chaves criptográficas	Analista de Segurança Pleno				2	Média	5	2	20
4	Definição e implementação de procedimentos de backup e restauração do gerenciamento de chaves restauração do gerenciamento de chaves	Definição de ativos e informações que serão objeto de backup;	Analista de Segurança	Relatório (documento) com as rotinas de backup definidas, evidências das configurações,	Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para definição e implementação de procedimentos de backup e restauração de chaves. O serviço poderá ser demandado após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.	Uma unidade de atividade por	8	Normal	1	1	8
		Definição de sazonalidade e estratégia (total, incremental, etc) a ser adotada, por ativo e informação objeto de backup.	Analista de Segurança				4	Normal	1	1	4
		Acompanhamento Da implantação das configurações definidas;	Analista de Segurança				4	Normal	1	1	4
		Acompanhamentode teste de restauração;	Analista de Segurança				4	Normal	1	1	4

		Definir agenda para testes de restauração sazonais	**Analista de Segurança**	**teste de restauração e agenda de testes de restauração**	**A infraestrutura de backup, incluindo softwares e armazenamento, bem como operação, são de responsabilidade da CONTRATANTE. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é de uma unidade por solução adquirida**	**solução adquirida**	**4**	**Normal**	**1**	**1**	**4**
	Serviço de Apoio Operacional da Solução	**Execução proativa de rotinas operacionais e atividades planejadas na console de gerenciamento centralizada e agentes;**	**Analista de Segurança Pleno**	**Relatório (documento) contendo relação de atividades executadas no período com respectivas evidências, incluindo data e hora do início da execução, término, nível de criticidade, demandante, data e hora da solicitação (quando houver).**	**Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para operação da solução por técnicos. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é a quantidade de meses da vigência contratual. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.**	**A quantidade de execuções desta atividade ao longo da vigência é a quantidade de meses da vigência contratual.**	**22**	**Média**	**12**	**2**	**528**
		Implementação de novas configurações e/ou ajustes na console de gerenciamento centralizada e agentes;	**Analista de Segurança Pleno**				**2**	**Média**	**12**	**2**	**48**
		Validação e correção, quando necessário, de cada procedimento realizado.	**Analista de Segurança Pleno**				**4**	**Média**	**12**	**2**	**96**
		Atendimento a solicitações da CONTRATANTE, tais como execução de atividades técnicas, configurações, validações, criação ou alteração de políticas, dentre outros, desde que diretamente relacionadas ao objeto contratado	**Analista de Segurança Pleno**				**2**	**Média**	**12**	**2**	**48**
		Validação e teste do procedimento de alta disponibilidade e replicação da solução;	**Analista de Segurança Pleno**				**5**	**Média**	**12**	**2**	**120**
		Serviço de Monitoramento Contínuo e Gestão de Alertas;	**Analista de Segurança Pleno**				**60**	**Média**	**12**	**2**	**1440**
		Gerenciamento do Ciclo de Vida de Chaves;	**Analista de Segurança Pleno**				**5**	**Média**	**12**	**2**	**120**
		Elaboração de documentos/relatórios técnicos	**Analista de Segurança Pleno**				**20**	**Média**	**12**	**2**	**480**
	Estimativa de quantidade total de UST a ser contratad a										**3.322**

1.9. Os serviços de operação assistida indicados no Catálogo de Serviços serão executados de acordo com a especificação indicada em cada item, evidenciado as atividades pormenorizadas para cada item.

1.10. O serviço de operação assistida, não obstante sua mediação em UST, se configura em atividade de demanda continuada relevante para a operacionalização da solução como um todo e, numa eventual prorrogação na contratação dos demais serviços de suporte, deverá permanecer disponibilizado, sendo também objeto da prorrogação contratual.

1.11. As atividades do Catálogo de Serviço representam mera expectativa, sendo admitida a execução de outras atividades que venham a ser necessárias, limitadas ao total de UST que venha a ser contratado.

1.12. ITEM 1 DO CATÁLOGO DE SERVIÇOS: Projeto Executivo

1.12.1. Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para elaboração de projeto executivo com vistas a operacionalizar a solução por completo, alinhada com os objetivos da contratação.

1.12.2. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é de uma unidade por solução adquirida.

1.12.3. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.

1.12.4. Atividades Contempladas:

- Elaboração de projeto executivo contendo minimamente:
- Levantamento de recomendações, riscos, premissas e restrições;
- Definição da equipe envolvida e respectivas funções de cada indivíduo;
- Elaboração de Plano de Comunicação operacional;
- Elaboração de matriz de responsabilidades;
- Mapeamento de objetivos a serem alcançados;
- Definição de atividades, prazos e responsáveis que serão realizadas ao longo do contrato.
- Definição de cronograma macro, abrangendo toda a vigência do contrato, detalhando atividades, prazos e responsáveis definidos;

- Definição de reuniões sazonais para ponto de controle entre as partes, a fim de avaliar, monitorar e ajustar o andamento das atividades previstas.

1.12.5. Dos Entregáveis:

- Projeto executivo (documento) consolidando as informações contempladas.

1.13. ITEM 2 DO CATÁLOGO DE SERVIÇOS: Parametrização da Console de Gerenciamento Centralizado

1.13.1. Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para parametrização da console de gerenciamento centralizado de chaves criptográficas.

1.13.2. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é de uma unidade por solução adquirida.

1.13.3. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.

1.13.4. Atividades contempladas:

- Implementação e validação da operação em alta disponibilidade;
- Definição e implementação de estratégia de perfis e funções de usuários;
- Criação de usuários;
- Integração com SIEM, caso a CONTRATANTE possua;
- Definição do rotacionamento de chaves criptográficas;
- Parametrização de alertas e notificações;

1.13.5. Dos Entregáveis:

- Relatório com evidências de todas as parametrizações executadas;

1.14. ITEM 3 DO CATÁLOGO DE SERVIÇOS: Parametrização de Agentes

1.14.1. Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para parametrização de agentes.

1.14.2. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é igual ao somatório de todos os agentes que compõem a aquisição.

1.14.3. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.

1.14.4. Atividades contempladas:

- Integração do agente com a console de gerenciamento centralizado;
- Definição de usuários e perfis, de acordo com o respectivo agente.
- Integração e comunicação com os ativos alvos de proteção, de acordo com o respectivo agente;
- Definição e implementação de rotinas operacionais, de acordo com o respectivo agente;
- Definição do rotacionamento de chaves criptográficas;

1.14.5. Dos Entregáveis:

1.15. ITEM 4 DO CATÁLOGO DE SERVIÇOS: Definição e implementação de procedimentos de backup e restauração do gerenciamento de chaves

1.15.1. Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para definição e implementação de procedimentos de backup e restauração de chaves.

1.15.2. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.

1.15.3. A infraestrutura de backup, incluindo softwares e armazenamento, bem como operação, são de responsabilidade da CONTRATANTE.

1.15.4. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é de uma unidade por solução adquirida.

1.15.5. Atividades contempladas:

- Definição de ativos e informações que serão objeto de backup;
- Definição de sazonalidade e estratégia (total, incremental, etc) a ser adotada, por ativo e informação objeto de backup.
- Acompanhamento da implantação das configurações definidas;
- Acompanhamento de teste de restauração;
- Definir agenda para testes de restauração sazonais;

1.15.6. Dos Entregáveis:

- Relatório (documento) com as rotinas de backup definidas, evidências das configurações, teste de restauração e agenda de testes de restauração.

1.16. ITEM 5 DO CATÁLOGO DE SERVIÇOS: Serviço de Apoio Operacional da Solução

1.16.1. Permite que a CONTRATANTE solicite através de ordem de serviço, apoio especializado para operação da solução por técnicos.

1.16.2. A métrica utilizada para estimar a quantidade de execuções do referido serviço ao longo da vigência é a quantidade de meses da vigência contratual.

1.16.3. O serviço poderá ser demandando após o término da instalação, configuração e entrega das licenças que compõem o objeto adquirido.

1.16.4. Atividades contempladas:

- Execução proativa de rotinas operacionais e atividades planejadas na console de gerenciamento centralizada e agentes;
- Implementação de novas configurações e/ou ajustes na console de gerenciamento centralizada e agentes;
- Validação e correção, quando necessário, de cada procedimento realizado.
- Atendimento a solicitações da CONTRATANTE, tais como execução de atividades técnicas, configurações, validações, criação ou alteração de políticas, dentre outros, desde que diretamente relacionadas ao objeto contratado.
- Validação e teste do procedimento de alta disponibilidade e replicação da solução;
- Serviço de Monitoramento Contínuo e Gestão de Alertas;
- Gerenciamento do Ciclo de Vida de Chaves;
- Elaboração de documentos/relatórios técnicos;

1.16.5. Dos Entregáveis:

- Relatório (documento) contendo relação de atividades executadas no período com respectivas evidências, incluindo data e hora do início da execução, término, nível de criticidade, demandante, data e hora da solicitação (quando houver).

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 25/11/2025, às 15:25, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 25/11/2025, às 15:58, 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 25/11/2025, às 15:58, 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 **Vania Lucia Barros Ventapane Soares**, **Técnico de Suporte, Computação e Processamento**, em 25/11/2025, às 18:33, 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 **119233835** e o código CRC **7F983C37**.

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 IV DO ESTUDO TÉCNICO PRELIMINAR

TESTE DE BANCADA

1. TESTE DE BANCADA

Será exigido do LICITANTE classificado em primeiro lugar Teste de Bancada para a demonstração de que a solução ofertada é compatível com as exigências técnicas necessárias e prescritas para este objeto, conforme os roteiro apresentados no Anexo IV, deste documento.

1.1. Prazos e Condições do Teste de Bancada

1.1.1. O referido LICITANTE será convocado no prazo máximo de até 10 (dez) dias úteis, a contar da aprovação da sua documentação de habilitação, para uma reunião (que poderá ocorrer em plataforma virtual), onde serão definidas as providências preparatórias do ambiente de teste. Nessa reunião o LICITANTE deverá informar os requisitos necessários para a instalação do ambiente de teste a serem disponibilizados pelo PRODERJ conforme entendimento durante a reunião. Entende-se por "requisitos necessários":

a) Disponibilização de máquinas virtuais e/ou estações de trabalho, projetor e link de internet;

b) Criação de VLAN's e/ou disponibilização de endereços IP;

c) Criação de usuários no AD e/ou modificações de regras de firewall, IPS, etc;

d) Disponibilização de periféricos, tais como: cabos, switches e outros componentes semelhantes não mencionados.

1.1.2. Nesta reunião o LICITANTE deverá, sob pena de desclassificação, entregar os documentos da(s) solução(ões) que permitam comprovar o atendimento aos requisitos técnicos constantes do Anexo I deste documento, apresentando no mínimo:

a) ID do requisito;

b) Descrição do requisito;

c) Nome do produto ofertado (modelo, marca e fabricante);

d) Nome do documento de referência onde é possível verificar evidência do atendimento do requisito;

e) Página do documento referência onde é possível verificar evidência do atendimentodo requisito;

f) Outras informações necessárias.

1.1.3. Até o prazo de 5 dias úteis após a realização da reunião preparatória, será divulgada a equipe técnica que avaliará a solução durante a sessão da prova. O teste será realizado no ambiente do PRODERJ, em um dos endereços abaixo mencionados a ser definido na reunião acima preparatória acima referida:

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: 20550013;

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

1.1.4. Admite-se, alternativamente, o uso de ambiente virtual do próprio LICITANTE ou do fabricante, para a comprovação das funcionalidades da solução ofertada, caso seja acordado na reunião preparatória. Nesta hipótese, o LICITANTE deverá disponibilizar o link de acesso ao acompanhamento da sessão virtual de demonstração até 3 (três) dias úteis antes da realização da sessão, para que o mesmo possa ser repassado em tempo hábil a todos os que acompanharão a sessão.

1.1.5. Em caso de não comparecimento à reunião (por problema único e exclusivo do LICITANTE) a prova acontecerá no ambiente padrão de teste do PRODERJ, em um dos endereços acima citados, sendo vedado ao LICITANTE reivindicar qualquer adaptação na infraestrutura oferecida.

1.1.6. O PRODERJ, por meio da Comissão Permanente de Licitação (Pregoeiro), dará publicidade, através do chat de mensagens do SIGA-RJ, da data de realização do teste que deverá ocorrer no prazo de 10 (dez) dias úteis após a realização da reunião preparatória. O referido prazo poderá ser prorrogado por igual período, mediante requisição fundamentada do LICITANTE.

1.1.7. Se o teste for realizado em ambiente do PRODERJ, o LICITANTE terá até as 17h do último dia útil anterior ao da realização do mesmo para providenciar a instalação do ambiente nas condições definidas na reunião.

1.1.8. A prova será realizada entre 10:00 e 18:00 horas (horário de Brasília), com intervalo de 1 hora para almoço, e poderá durar de 1 a 5 dias úteis.

1.2. **Possibilidade e forma de participação dos interessados**

1.2.1. Os outros licitantes que tenham participado da etapa competitiva e demais interessados que desejem acompanhar a sessão, poderão indicar um representante para acompanhamento, devendo para tanto enviar para o e-mail da Comissão Permanente de Licitação (cdl@proderj.rj.gov.br) até as 16hs do último dia útil que antecede a sessão de teste. No e-mail deverão constar: dados da empresa interessada (nome e contato), de seu representante (nome e contato) para o devido credenciamento.

1.3. **Roteiro e critérios de avaliação**

1.3.1. No dia de realização do teste, o LICITANTE, bem como os demais interessados em acompanhar, deverão chegar ao local indicado com antecedência mínima de 30 minutos.

1.3.2. Durante a prova poderá ser feito questionamento, exclusivamente pelos representantes do PRODERJ à proponente, permitindo a verificação dos requisitos estabelecidos.

1.3.3. Após a prova será emitido, via Sistema Eletrônico de Informações, relatório descrevendo ostestes realizados e a conclusão sobre a aprovação da proposta ou desclassificação bem como eventuais ocorrências ou manifestações de quaisquer dos presentes na sessão. Para a solução ser considerada apta para ser contratada pela Administração, todos os requisitos de software que constam no presente documento e seu anexo de especificações técnicas, deverão ser considerados ATENDIDOS.

1.3.4. Será desclassificada a licitante que for convocada para o Teste de Bancada e não demonstrar a compatibilidade de seu produto conforme as especificações técnicas exigidas ou não comparecer no dia marcado sob qualquer pretexto.

1.3.5. Em caso de desclassificação no Teste de Bancada deverá ser convocada o próximo licitante na ordem de classificação, resguardadas todas as condições e prazos previstos neste tópico.

1.4. **Responsabilidades**

1.4.1. Os custos para a demonstração da solução são de responsabilidade do LICITANTE e em hipótese alguma caberá qualquer tipo de indenização.

1.4.2. O LICITANTE deverá disponibilizar ao menos 01 (um) técnico que se responsabilizará pela instalação do software da solução, caso o teste seja realizado utilizando a infraestrutura do PRODERJ.

1.4.3. A disponibilização de equipamentos, sistemas, demais materiais e/ou acessórios necessários ao ambiente de demonstração durante a prova não informados pelo LICITANTE na reunião preparatória citada no subtópico 1.1 deste documento são de inteira responsabilidade do LICITANTE.

1.4.4. Ficará sob responsabilidade do PRODERJ o resguardo dos itens eventualmente entregues pelo licitante para a avaliação no Teste de Bancada, devendo restituí-los ao final nas condições recebidas, resguardados eventuais consumos decorrentes da realização da prova.

1.4.5. A desmobilização do ambiente é de responsabilidade do LICITANTE, que após a finalização do Teste de Bancada terá até 72 (setenta e duas) horas úteis para retirar das dependências do PRODERJ os itens por ele instalados para composição do ambiente de teste, sob pena de destinação na forma do Decreto 48.816/2023, art. 21, §3º:

> "As amostras, provas de conceito ou objetos a serem submetidos a exame de conformidade em depósito nos órgãos e entidades estaduais, sem que haja interesse dos licitantes em sua retirada, devem, após comunicação dos licitantes proprietários e perdurando o desinteresse, ser considerados como coisas abandonadas, com perda da propriedade, conforme o disposto no Art. 1.263 e inciso III do Art. 1.275 da Lei nº 10.406 , de 10 de janeiro de 2002 e poderão ser incorporados ao patrimônio do Estado ou formalmente descartados."

2. CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS:

2.1. Sobre o gerenciamento de chaves criptográficas e criptografia:

a) Deverá demonstrar que a solução ofertada estabelece um modelo de proteção para informações de tal forma que o dado seja devidamente criptografado no sistema de arquivos;

b) Deverá demonstrar que os dados não podem ser acessados fora do ambiente gerenciado pela plataforma de segurança;

c) Deverá demonstrar que a solução ofertada protege sistemas de dados estruturado (bancos de dados) e sistemas de dados não estruturado;

d) Deverá demonstrar que a solução ofertada suporta pelo menos os sistemas operacionais Microsoft Windows Server e Linux;

e) Deverá demonstrar que a solução ofertada suporta pelo menos dois dos bancos de dados a serem definidos para efeito de teste: Oracle, MS-SQL, MySQL, Mongo DB, NoSQL, Teradata, SAP Hana e Hadoop Distributed arquivos;

f) Deverá demonstrar que a solução ofertada possui uma console de gerenciamento centralizado;

g) Deverá demonstrar que a console de gerenciamento oferece recursos para proteger e controlar o acesso a bancos de dados e arquivos;

h) Deverá demonstrar que a console de gerenciamento permite o gerenciamento centralizado de todos os agentes de criptografia, suas chaves de criptografia, políticas de configuração, publicação e controle de acesso dos dados;

i) Deverá demonstrar que a console de gerenciamento centralizado suporta agentes para as funcionalidades de criptografia transparente para servidores de arquivos controlando o acesso e oferecendo registros de auditoria de acesso sem impactar nas aplicações, base de dados ou infraestrutura;

j) Deverá demonstrar a integração com os sistemas de gerenciamento de logs;

k) Deverá demonstrar a Tokenização e mascaramento dinâmico de dados;

l) Deverá demonstrar que é capaz de ser configurada em alta disponibilidade (HA);

m)Deverá demonstrar que os agentes instalados nos servidores operam de forma autônoma mesmo com a perda de comunicação com a console;

n) Deverá demonstrar que os agentes fazem a rotação/mudança de chaves sem causar

indisponibilidade ou degradação nos servidores de dados;

o) Deverá demonstrar que suporta o gerenciamento em estrutura de multi-tenant com suporte a configuração de segurança de vários domínios;

p) Deverá demonstrar que o gerenciamento via interface Web e inserir comandos via interface de linha de comando (CLI);

q) Deverá demonstrar que requer autenticação de usuário e senha;

r) Deverá demonstrar a realização de cópias de segurança (Backup) de suas configurações.

2.2. **Sobre os agentes de proteção de dados para banco de dados:**

a) Deverá demonstrar que sua implementação não exige qualquer alteração no banco de dados ou na aplicação;

b) Deverá demonstrar que a implementação não gera carga incremental, típica em servidores, de mais de 5%;

c) Deverá demonstrar que além de criptografar o conteúdo do banco de dados, os agentes são capazes de criptografar arquivo, volume ou diretório desses servidores;

d) Deverá demonstrar que os agentes registram e rastreiam o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso;

e) Deverá demonstrar que as políticas de controle de acesso podem ser aplicadas mesmo aos usuários privilegiados do sistema e estes não terão autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio;

f) Deverá demonstrar que os registros (logs) de atividade do usuário são enviados para um servidor de syslog;

g) Deverá demonstrar que todas as tentativas de acesso são registradas;

h) Deverá demonstrar as políticas de acesso baseadas em função.

2.3. **Sobre os agentes de proteção de dados para servidores de arquivos (file server):**

a) Deverá demonstrar que oferece suporte a sistemas operacionais Microsoft e Linux;

b) Deverá demonstrar que a implementação não exige qualquer alteração no servidor de arquivo ou processo para manuseio do dado pelo usuário final;

c) Deverá demonstrar que é capaz de criptografar arquivo, volume ou diretório;

d) Deverá demonstrar que é capaz de registrar e de rastrear o acesso dos usuários de sistema aos arquivos e ser capaz de bloquear ou restringir este acesso;

e) Deverá demonstrar que as políticas de controle de acesso podem ser aplicadas mesmo aos usuários privilegiados do sistema e estes não deverão possuir autoridade para desfazer a política de acesso na tentativa de elevar novamente seu privilégio;

f) Deverá demonstrar a integração com um servidor de syslog;

g) Deverá demonstrar que registra todas as tentativas de acesso;

h) Deverá demonstrar que os usuários privilegiados não possuem acesso a dados em texto não criptografado.

2.4. **Sobre os agentes de proteção de dados para aplicações web:**

a) Demonstrar a Tokenização com mascaramento dinâmico, para promover a anonimização de dados;

b) Demonstrar a interface REST API com chamadas individuais e em lote;

c) Demonstrar a geração de Tokens Aleatórios;

d) Demonstrar o gerenciamento de chaves e políticas;

e) Demonstrar o suporte a dados numéricos e alfanuméricos;

f) Demonstrar a criação de tokens em formatos numéricos, de texto e de data para aplicativos únicos ou múltiplos;

g) Apresentar a configuração de grupos de usuários para decidir quais informações são exibidos para grupos específicos;

h) Demonstrar que a restrição do acesso a ativos confidenciais não altera os esquemas do banco de dados e nem causam interrupções;

i) Demonstrar que as chaves criptográficas utilizadas para tokenização são criadas na console de gerenciamento centralizado e podem ser utilizadas de forma nativa pelo agente de proteção de dados em aplicações web, ou seja, sem o uso de scripts, softwares de terceiros e códigos;

j) Demonstrar a criação de usuários para tokenização, a escolha de quais chaves criptográficas poderão ser usadas por um dado usuário e as opções de permissão para tokenizar e detokenizar informações;

k) Demonstrar requisições REST para tokenizar e detokenizar uma informação;

l) Demonstrar que após a remoção de chave criptográfica na console de gerenciamento, não é mais possível realizar ações de tokenição e detokenização com o usuário associado à chave.

2.5. **Sobre os agentes para compartilhamento seguro de base de dados:**

a) Deverá demonstrar o mascaramento dos dados sensíveis através da criptografia de uma determinada tabela e coluna;

b) Deverá demonstrar que a solução é transparente para a aplicação ou banco de dados com acesso via conexão ODBC;

c) Demonstrar o processo de compartilhamento seguro de base de dados em banco SQL SERVER, executando Tokenização de ao menos 3 colunas de uma tabela usando chave criptográfica gerada na console de gerenciamento centralizado. Exportação para arquivo CSV e Exportação para outro banco de dados SQL SERVER.

2.6. **Sobre os agentes de proteção de dados para Contêineres:**

a) Demonstrar em container a tentativa de acesso a um arquivo criptografado;

b) Demonstrar na console de gerenciamento centralizada a alteração na política de acesso, de modo que o usuário usado no primeiro passo não possa mais acessar o mesmo arquivo criptografado;

c) Demonstrar em container nova tentativa de acesso ao arquivo criptografado, onde o resultado esperado é que seja negado;

d) Demonstrar no orquestrador do container que a imagem não foi alterada, ou seja, não houve instalação de software adicional ou scripts.

2.7. **Sobre os agentes para proteção de dados na Nuvem:**

a) Demonstrar na console de gerenciamento centralizado, a associação de agentes de gestão de chaves na nuvem à uma conta no provedor AWS e outra conta no provedor AZURE;

b) Demonstrar a capacidade de gerenciamento de chaves de diferentes provedores de nuvem a partir de uma única janela do navegador, incluindo as respectivas contas de cada provedor;

c) Demonstrar o sincronismo de chaves ocorrido entre os provedores de nuvem AWS e AZURE e a console de gerenciamento centralizada;

d) Demonstrar na console do provedor de nuvem a existência de chave criptográfica criada na console de gerenciamento centralizado;

e) Demonstrar na console de gerenciamento centralizado o rotacionamento automático de chaves criptográficas utilizadas nos provedores de nuvem.

2.8. **Sobre os agentes para proteção de chave local:**

a) Demonstrar o registro de aplicativo cliente na console de gerenciamento centralizado utilizando protocolo KMIP;

b) Demonstrar na console de gerenciamento centralizado as chaves criptográficas geradas pelos aplicativos clientes registrados;

c) Demonstrar que após a exclusão de chave criptográfica na console de gerenciamento centralizado, o aplicativo cliente perdeu acesso ao recurso criptografado.

2.9. **Sobre os agentes para Descoberta e Classificação de Dados:**

a) Demonstrar que o agente de descoberta e classificação de dados possui diferentes perfis pré-definidos, que incluem padrões regulatórios, como a LGPD;

b) Demonstrar que o agente de descoberta e classificação de dados possui categorias de nível de sensibilidade (Restrito, Privado, Interno e Público);

c) Demonstrar com o agente de descoberta e classificação de dados uma varredura em busca de CPF (cadastro de pessoa física) ou PASSAPORTE que ocorra de forma simultânea em um banco de dados SQL e um diretório com arquivos distintos (PDF, XLS, DOC, JPG e PNG);

d) Demonstrar que o agente de descoberta e classificação de dados permite a criação de políticas para classificação de dados baseado na LGPD;

e) Demonstrar na console de gerenciamento centralizado a capacidade de proteger de forma automática, através de criptografia transparente, arquivos que possuam dados classificados como pessoais ou sensíveis encontrados em uma varredura do agente de descoberta e classificação de dados.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 25/11/2025, às 15:25, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022 e no art. 4º do Decreto nº 48.013, de 04 de abril de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor-Chefe**, em 25/11/2025, às 15:58, 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 25/11/2025, às 15:58, 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 **Vania Lucia Barros Ventapane Soares**, **Técnico de Suporte, Computação e Processamento**, em 25/11/2025, às 18:33, 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 **119235090** e o código CRC **B745EE3A**.

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