



TERMO DE REFERÊNCIA

1. JUSTIFICATIVA DA NECESSIDADE E DO TIPO DE SOLUÇÃO ESCOLHIDA

1.1. Justificativa da Necessidade

Conforme detalhadamente descrito no Estudo Técnico Preliminar (ETP), a meta estabelecida pela Secretaria de Estado de Transformação Digital - SETD para a plena digitalização dos serviços, com gradual extinção do "atendimento de balcão", até o final de 2025, na forma do Decreto Estadual nº 48.671/2023, faz-se necessário a adoção de solução de proteção e melhoria de performance das aplicações web, de forma a resguardar o pleno funcionamento dos serviços aos cidadãos, ante ao crescente número de ocorrência de ataques cibernéticos. A pretendida contratação se justifica, inclusive, por conta de ataques do tipo "negação de serviços/DoS", sofridos recentemente na rede CONECTA/RJ, como podemos ver nos prints do último Relatório de Segurança emitido pelo SOC da Claro no mês de Dezembro/2024, mostrados abaixo:

1 - Tentativas de Ataques por Severidades

Ameaças por Severidades

High	376,609,054
Critical	1,493,948
Info	768,985
Low	624,166
Medium	102,453



Fig. 1: Ameaças de nível alto foram predominantes no período. Fonte: Relatório SOC/Claro, Dez/2024.

Top 10 Ataques Bloqueados

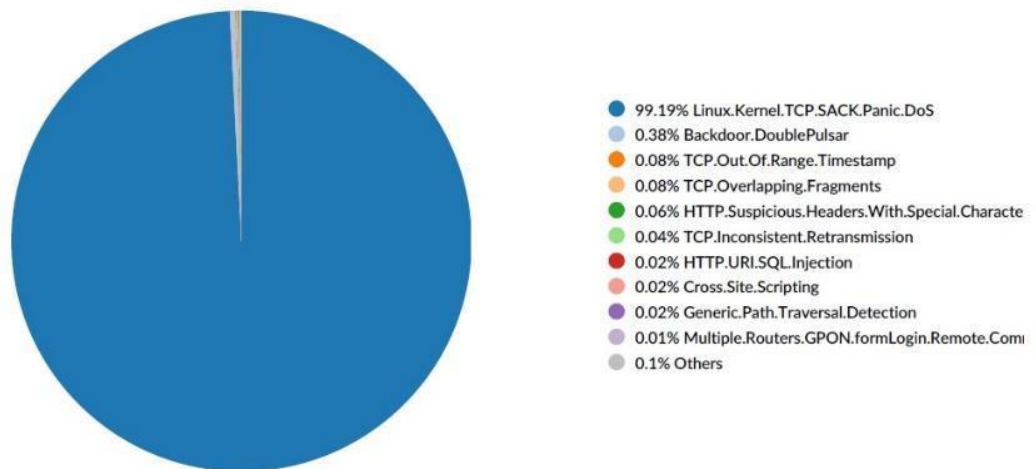


Fig. 2: Ataques de negação de serviços representaram a maioria absoluta dos métodos empregados no período. Fonte: Relatório SOC/Claro, Dez/2024.

1.2. Em virtude das atribuições do PRODERJ, autarquia responsável por manter e operar a Tecnologia da Informação e Comunicação 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, e, também, a sua responsabilidade em prover serviços de Internet à Administração Pública, tais como correio eletrônico, consultoria, desenvolvimento e hospedagens de páginas, portais, intranets e extranets, fica a seu cargo a manutenção do Portal Único RJ Digital (art. 7º do Decreto nº 48.671/2023), com a unificação de informações e serviços prestados pelos órgãos e entidades do Poder Executivo do Estado do Rio de Janeiro.

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

1.4. Fim de prevenir invasões e diversos tipos de ataques que podem causar falhas de segurança e perda de performance às aplicações, comprometendo assim informações de extrema relevância, bem como a experiência do usuário, o PRODERJ vem buscando mecanismos de inspeção, detecção e bloqueio de ameaças de forma automatizada e segura.

1.5. Um dos modos mais eficazes de evitar roubo de informações e ataques a sites e aplicações web é através do Web Application and API Protection (WAAP), um filtro que inspeciona o tráfego http/https antes de chegar ao aplicativo, site ou através de requisições API, protegendo os servidores através do bloqueio de ameaças que podem danificar a funcionalidade do site ou comprometer os dados. Paralelamente, e de maneira independente, a solução de Application Delivery Controller (ADC) fará o controle e melhoria de performance das aplicações por meio de algoritmos de balanceamento, assim permitindo um funcionamento mais dinâmico para os usuários.

1.6. Essa ferramenta contribuirá para o atendimento da Lei Federal nº 13.709/2018, Lei Geral de Proteção a Dados (LGPD), que intensifica a obrigatoriedade de proteção e privacidade dos dados dos titulares, no nosso caso, os cidadãos, reforçando a necessidade do PRODERJ 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.

1.7. Pretende-se também atender uma das determinações do Decreto Estadual 47.278/2020, alterado pelas disposições do Decreto 48.997/2024, pelo qual o PRODERJ deverá conduzir e disponibilizar as atas de registro de preços e contratos corporativos para suprir itens relativos à TIC aos Órgãos e entidades do Estado.

1.8. A presente contratação busca, assim, o robustecimento da segurança da informação nas aplicações WEB do PRODERJ, bem como dos diversos órgãos do Governo do Estado com sistemas hospedados na infraestrutura desta Autarquia.

1.9. Soluções de proteção e otimização da aplicação web abrangem ferramentas de Web Application and API Protection (WAAP) e de Application Delivery Controller (ADC).

1.10. Web Application and API Protection (WAAP) consiste em um filtro que inspeciona o tráfego http/https antes de chegar ao aplicativo ou site, protegendo os servidores através do bloqueio de ameaças que podem danificar a funcionalidade do sistema ou comprometer os dados.

1.11. Application Delivery Controller (ADC) consiste em um dispositivo cujo propósito é aperfeiçoar a entrega, disponibilidade e desempenho de aplicações web, através do balanceamento de carga das aplicações entre os servidores.

1.12. As soluções de WAAP e ADC diferenciam-se, essencialmente, pelo fato da primeira ser especializada em garantir a segurança das aplicações web e API (prevenção de ataques como: SQL injection, XSS, DDoS), enquanto a segunda trabalha com a otimização da entrega das aplicações, através do balanceamento de carga dos servidores e das aplicações.

1.13. As soluções de WAAP e ADC desempenham papel fundamental na manutenção e disponibilidade adequada aos serviços e à continuidade das operações institucionais e corporativas, apoiando as divisões de infraestrutura e de segurança da informação desta Autarquia de forma a manter suas aplicações web íntegras, seguras e disponíveis.

1.14. **Justificativa do Tipo de Solução Escolhida**

1.14.1. A partir do levantamento comparativo feito no ETP, das soluções oferecidas pelo mercado, optou-se por aquela que oferta a solução WAAP em duas modalidades de contratação que combina a aquisição de hardware e a subscrição de software. Desta forma, o PRODERJ terá condições plenas de proteger e otimizar suas aplicações web de maneira centralizada, estejam elas on premise ou em nuvem.

1.14.2. Desse modo, a oferta da solução WAAP, também via subscrição, estará em um item separado dos appliances, contendo ao menos um item para a subscrição do WAAP, e outro contendo uma franquia adicional para tráfego de dados, caso a franquia mensal pré definida seja ultrapassada, uma vez que o PRODERJ ainda não possui visibilidade sobre a volumetria de dados trafegados pelas aplicações, o que será possível com o uso das referidas ferramentas.

2. **DEFINIÇÃO DO OBJETO**

2.1. Registro de Preços para aquisição de uma solução Web Application and API Protection – WAAP, incluindo a aquisição perpétua de hardware e software, com garantia de 36 (trinta e seis) meses, bem como a prestação de serviço de subscrição de software por 12 (doze) meses, com instalação/configuração, suporte técnico e treinamento da solução (LOTE I); e Registro de Preços para aquisição de solução Application Delivery Controller – ADC, incluindo a aquisição perpétua de hardware e software, com garantia de 36 meses, bem como a prestação de serviço de instalação/configuração, suporte técnico e treinamento da solução (LOTE II), conforme especificações e quantidades estabelecidas neste Termo de Referência e nos requisitos da contratação descritos no Estudo Técnico Preliminar, conforme condições definidas no ANEXO I, deste documento.

3. **INSTRUMENTOS DE PLANEJAMENTO**

3.1. A solução pretendida está prevista no Plano de Contratações Anual (PCA) desta autarquia, conforme abaixo:

3.1.1. **ID PCA no PNCP:** 42498600000171-0-000041/2025

3.1.2. **Data de publicação no PNCP:** 01/08/2024

3.1.3. **ID do item no PCA:** 24357, 24361, 23828, 24354, 24355 e 24356 (itens 1 a 6 do Lote I respectivamente) / 24358 e 24359 (itens 1 e 2 do Lote II)

3.2. **Alinhamento Estratégico**

A solução pretendida está prevista no Plano Estratégico e Diretor de Tecnologia da Informação e Comunicação - PEDTIC (91818377, p 47 e 48) do PRODERJ, conforme demonstrado abaixo:

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

4. **ESPECIFICAÇÃO DO BEM OU DO SERVIÇO CONFORME CATÁLOGO ELETRÔNICO DE PADRONIZAÇÃO DE COMPRA**

4.1. **WAAP – LOTE I**

WAAP – LOTE I						
Item	ID SIGA	ID PCA-PNCP	Descrição	Métrica	Quantidade	Forma de quantificação
1	191788	24357	Appliance de Web Application and API Protection (WAAP) - Hardware Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	2	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
2	191799	24361	Appliance de Web Application and API Protection (WAAP) - Virtual Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	2	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
3	186917	23828	Treinamento operacional para appliances WAAP	Turma	1	Uma turma dá direito ao treinamento de 8 alunos.
4	186914	24354	Subscrição de solução para proteção em nuvem (SaaS), incluindo instalação, configuração e suporte técnico por 12 meses.	Anuidade	1	1 anuidade inclui: franquia mensal de 2.5 Terabytes de tráfego limpo, podendo ser consumido em até 25 aplicações (distribuídas em até 150 servidores).
5	187045	24355	Franquia adicional de tráfego limpo para o Item 4	TeraByte (TB)	12	A métrica do item é por terabyte, ou seja, basta informar a quantidade de terabytes adicionais que serão necessários.
6	186921	24356	Treinamento operacional para WAAP SaaS	Turma	1	Uma turma dá direito ao treinamento de 8 alunos.

4.2. ADC – LOTE II

tem	ID SIGA	ID PCA-PNCP	Descrição	Métrica	Quantidade	Forma de quantificação
1	191789	24358	Appliance de Controle de Entrega de Aplicação (ADC) e Balanceamento Dinâmico de Carga, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	4	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
2	188007	24359	Treinamento operacional para ADC	Turma	1	Uma turma dá direito ao treinamento de 8 alunos.

5. DESCRIÇÃO PORMENORIZADA CONSIDERANDO TODO O CICLO DE VIDA DO OBJETO A SER CONTRATADO

5.1. O ciclo de vida das soluções tratadas neste documento refere-se ao período durante o qual o fabricante fornece suporte e atualizações para o produto.

5.2. A descrição detalhada do objeto desta contratação está descrita no Anexo I - Especificações Técnicas do Objeto, deste Termo de Referência.

6. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

6.1. Registro de Preços para aquisição de uma solução Web Application and API Protection – WAAP, incluindo a aquisição perpétua de hardware e software, com garantia de 36 (trinta e seis) meses, bem como a prestação de serviço de subscrição de software por 12 (doze) meses, com instalação/configuração, suporte técnico e treinamento da solução (LOTE I); e Registro de Preços para aquisição de solução Application Delivery Controller – ADC, incluindo a aquisição perpétua de hardware e software, com garantia de 36 meses, bem como a prestação de serviço de instalação/configuração, suporte técnico e treinamento da solução (LOTE II), conforme especificações e quantidades estabelecidas neste Termo de Referência e nos requisitos da contratação descritos no Estudo Técnico Preliminar, conforme condições definidas no ANEXO I, deste documento.

6.2. Natureza do Objeto

6.2.1. Os itens que integram os lotes de objetos previstos neste documento 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 BENS e SERVIÇOS COMUNS ou usuais de mercado.

6.2.2. Os Objetos constituem soluções em TIC, parceladas em dois lotes que agregam soluções de WAAP (Lote I) e de ADC/Load Balance (Lote II), bem como os respectivos cursos de capacitação e treinamento, observados os seguintes aspectos:

- I - Os itens 1 e 2 do Lote I e o item 1 do Lote II são medidos em unidades e correspondem a aquisição de bens (compra);
- II - O item 4 do Lote I é medido por anuidade e corresponde a serviço de natureza contínua (subscrição/ licença de uso de software);
- III - O item 5 do Lote I é medido por terabyte e corresponde a serviço de natureza contínua (franquia);
- IV - Os itens 3 e 6 do Lote I e o item 2 do Lote II são medidos por turma (até 8 alunos), e correspondem a serviços por escopo (treinamento) a ocorrerem sob demanda.

7. MODELO DE EXECUÇÃO DO OBJETO

7.1. As aquisições dos itens 1 e 2 do Lote I e do item 1 do Lote II tem por objeto o atendimento de uma só vez, conforme Art 6º, X, da Lei nº 14.133/2021;

7.2. O regime de execução aplicável aos serviços dos itens 3, 4 e 6 do Lote I e do item 2 do Lote II será Empreitada por preço global, conforme Art. 6º, XXIX da Lei nº 14.133/2021.

7.3. O regime de execução aplicável ao serviço do item 5 do Lote I será Empreitada por preço unitário, conforme Art. 6º, XXVIII da Lei nº 14.133/2021..

8. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

8.1. Tendo em vista incentivar a competitividade no certame, optou-se por separar as tecnologias de WAAP e ADC em lotes distintos. No primeiro lote, constam duas modalidades de contratação para WAAP: aquisição de hardware e subscrição de software, sendo que ambas as modalidades de contratação acompanham itens de treinamentos opcionais. Tal escolha possibilita a integração, desde que sejam do mesmo fabricante, entre os appliances WAAP e o serviço WAAP SaaS, proporcionando uma visão completa dos aspectos de segurança nas aplicações web do PRODERJ, estejam elas em ambiente on premise ou cloud. Já o segundo lote, será para aquisição de hardware ADC, com seu respectivo treinamento. Tal definição é corroborada pelo fato de, neste objeto, não ser necessária a compatibilização tecnológica entre os dois lotes.

8.2. 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.

8.3. O parcelamento do objeto em dois lotes distintos é técnica e economicamente indicado, tendo em vista a já mencionada interoperabilidade entre as soluções WAAP, e a facilidade de uso e operação, recomenda-se que elas sejam fornecidas por um único fabricante, enquanto o equipamento ADC do lote II funciona de maneira independente das soluções WAAP, e por este motivo, não necessita figurar no mesmo lote.

8.4. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes das soluções e melhor gerenciamento do contrato.

8.5. O objeto ora pretendido se configura em uma solução de TI composta, conforme a infraestrutura do PRODERJ, por mais de um item e está disposta em dois lotes distintos.

8.6. O agrupamento dos itens levou ainda em consideração questões técnicas, bem como o ganho de economia em escala, sem prejuízo a ampla competitividade, uma vez que existem no mercado várias empresas com capacidade de fornecer os produtos e serviços na forma em que estão agrupados neste documento, bem como para facilitar a execução e fiscalização do contrato, propiciando maior nível de controle pela Administração, sendo prática comum reconhecida pelo mercado.

8.7. Na tabela abaixo, breve análise de cada item dos lotes que irão compor o Objeto:

WAAP – LOTE I				
Item	Descrição	Métrica	Justificativa do Item	Forma de quantificação
1	Appliance de Web Application and API Protection (WAAP) - Hardware Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	Este item corresponde ao appliance físico da solução WAAP. O equipamento deve fazer parte do cluster principal/ativo.	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
2	Appliance de Web Application and API Protection (WAAP) - Virtual Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	Este item corresponde ao appliance virtualizado da solução WAAP. O equipamento deve fazer parte do cluster secundário/standby.	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
3	Treinamento operacional para appliances WAAP	Turma	Serviço opcional de treinamento na solução. Recomendável, dada a complexidade da ferramenta.	Uma turma dá direito ao treinamento de 8 alunos.
4	Subscrição de solução para proteção em nuvem (SaaS), incluindo instalação, configuração e suporte técnico por 12 meses.	Anuidade	Este item corresponde à solução para proteção das aplicações da Autarquia hospedadas em nuvens públicas.	1 anuidade inclui: franquia mensal de 2.5 Terabytes de tráfego limpo, podendo ser consumido em até 25 aplicações (distribuídas em até 150 servidores).
5	Franquia adicional de tráfego limpo para o Item 4	TeraByte (TB)	Este item corresponde a franquia extra de tráfego limpo, a ser utilizado juntamente com a subscrição do item 4, caso a franquia mensal de 2.5 TB não seja suficiente.	A métrica do item é por terabyte, ou seja, basta informar a quantidade de terabytes adicionais que serão necessários.

6	Treinamento operacional para WAAP SaaS	Turma	Serviço opcional de treinamento na solução. Recomendável, dada a complexidade da ferramenta.	Uma turma dá direito ao treinamento de 8 alunos.
ADC – LOTE II				
Item	Descrição	Métrica	Justificativa do Item	Forma de quantificação
1	Appliance de Controle de Entrega de Aplicação (ADC) e Balancamento Dinâmico de Carga, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	Este item corresponde a solução para a melhoria da performance e entrega das aplicações, a ser utilizado em segmentos onde a entrega da aplicação seja prioritária.	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
2	Treinamento operacional para ADC	Turma	Serviço opcional de treinamento na solução. Recomendável, dada a complexidade da ferramenta.	Uma turma dá direito ao treinamento de 8 alunos.

9. PRAZOS DE INÍCIO E TÉRMINO DA PRESTAÇÃO DO SERVIÇO OU DE EXECUÇÃO DO OBJETO CONTRATUAL

9.1. Prazo do contrato e possibilidade de prorrogação

9.1.1. O prazo de vigência do contrato para os itens 1 e 2 do Lote I e do item 1 do Lote II será de 180 (cento e oitenta) dias corridos, contado da data da divulgação no Portal Nacional de Contratações Públicas. 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.

9.1.2. O prazo de vigência do contrato para os itens 4 e 5 do Lote I será de 12 (doze) meses, contados da data da divulgação no Portal Nacional de Contratações Públicas, podendo ser prorrogado, sucessivamente, até o máximo de 10 (dez) anos, na forma dos arts. 106 e 107 da Lei nº 14.133/2021, desde que observadas as condições previstas no Contrato, e mediante a celebração de termo aditivo.

9.1.3. O prazo de vigência do contrato para os itens 3 e 6 do Lote I e do item 2 do Lote II será de 12 (doze) meses, contados da data da divulgação no Portal Nacional de Contratações Públicas. 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.

9.2. Prazo e condições para a entrega do objeto

9.2.1. Forma de Entrega

9.2.1.1. A entrega dos bens de aquisição perpétua (itens 1 e 2 do Lote I (WAAP) e item 1 do Lote II (ADC) do objeto, em parcela única, se dará através da entrega dos respectivos equipamentos (resguardado o período de instalação e configuração para fins de recebimento definitivo).

9.2.1.2. A entrega dos serviços de treinamento (itens 3 e 6 do Lote I (WAAP) e item 2 do Lote II (ADC), sob demanda, acontecerá através do portal de treinamentos da contratada ou que esta venha a disponibilizar.

9.2.1.3. A entrega dos serviços de subscrição (item 4 do Lote I (WAAP), em parcela única, se dará de forma virtual, via liberação do acesso na plataforma da solução.

9.2.1.4. A entrega dos serviços de franquia (item 5 do Lote I (WAAP), sob demanda, se dará de forma virtual, na plataforma da solução, onde constará o consumo da franquia excedente utilizada.

9.2.2. Prazo de Entrega

9.2.2.1. Os cronogramas para entrega dos objetos, considerados os lotes do objeto e contados em dias úteis, será conforme as tabelas abaixo:

I - Entrega do Lote I (WAAP, somente itens 1, 2 e 3) e Lote II (ADC):

Prazo	Marco para contagem do prazo	Atividades	Responsável
03	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Emissão da "Ordem de Fornecimento"	Contratante
15	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Realização da Reunião Kick-Off prevista no subtópico " Requisitos de Projeto e de Implementação " previsto neste documento	Contratante e Contratada
10	Emissão da "Ordem de Fornecimento"	Entrega das soluções componentes do objeto (hardware + software + licença padrão)	Contratada
35	Reunião Kick-Off	Instalação completa das soluções WAAP e/ou ADC (incluindo configurações, regras, políticas, etc.) com a entrega do Relatório de Cumprimento do Objeto previsto no subtópico 11.1, inciso IV deste documento.	Contratada
20	Emissão da Ordem de Serviço (Treinamento)	Início do treinamento da solução	Contratada
10	Conclusão do Treinamento	Entrega do Relatório de Cumprimento do Objeto previsto no subtópico 11.1, inciso IV deste documento.	Contratada
02	Entrega do Relatório de Cumprimento do Objeto previsto no subtópico 10.1, inciso IV deste documento.	Emissão do Termo de Recebimento Provisório (para o serviço de treinamento)obs: para os itens 1 e 2 do Lote I - WAAP e para o item 1 do Lote II - ADC, o recebimento é sumário.	Contratante
20	Emissão do Termo de Recebimento Provisório (para o serviço de treinamento) ou do recebimento sumário (para os itens 1 e 2 do Lote I - WAAP e para o item 1 do Lote II - ADC)	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura, resguardadas as disposições do subtópico 11.4 deste documento.	Contratante

II - Entrega do Lote I - WAAP (somente itens 4, 5 e 6):

Prazo	Marco para contagem do prazo	Atividades	Responsável
03	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Emissão da "Ordem de Serviço" (subscrição e franquia)	Contratante
15	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Realização da Reunião Kick-Off prevista no subtópico " Requisitos de Projeto e de Implementação " previsto neste documento	Contratante e Contratada
03	Reunião Kick Off	Liberação do acesso da Contratante na plataforma SaaS da solução	Contratada
05	Reunião Kick Off	Início da implementação do escopo inicial de aplicações web que foram indicados pela Contratante na reunião de "Kick-Off".	Contratada
20	Reunião kick-off	Conclusão da implementação da configuração inicial básica da solução (entrega definitiva) e Entrega do Relatório de Cumprimento do Objeto previsto no subtópico 11.1, inciso IV deste documento.	Contratada
20	Emissão da Ordem de Serviço (Treinamento)	Início do treinamento da solução	Contratada
02	Entrega do Relatório de Cumprimento do Objeto previsto no subtópico 11.1, inciso IV deste documento	Emissão do Termo de Recebimento Provisório	Contratante
20	Emissão do Termo de Recebimento Provisório	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura, resguardadas as disposições do subtópico 11.4. deste documento.	Contratante

10. INDICAÇÃO DOS LOCAIS DE ENTREGA DOS PRODUTOS OU DA EXECUÇÃO DOS SERVIÇOS

10.1. A entrega dos bens de aquisição perpétua do objeto (itens 1 e 2 do Lote I (WAAP) e item 1 do Lote II (ADC)), bem como eventuais atendimentos presenciais de suporte técnico, será realizada no endereço indicado pela Contratante.

- 10.2. No caso do PRODERJ, a entrega ocorrerá em um dos três endereços abaixo, a definir no kick off:
- a) Data Center – Universidade do Estado do Rio de Janeiro (UERJ). End.: R. São Francisco Xavier 524, 2º andar, bloco “F”, Maracanã, Rio de Janeiro – RJ, CEP: 20550-013;
 - b) Data Center – Centro Integrado de Comando e Controle (CICC). End.: Rua Carmo Neto s/nº, Cidade Nova, Rio de Janeiro – RJ – CEP 20210-051; ou
 - c) Sede – Centro de Tecnologia de Informação e Comunicação do Governo do Estado do Rio de Janeiro (PRODERJ). End.: R. da Conceição 69, 24º e 25º andar, Centro, Rio de Janeiro – RJ CEP 20051-011
- 10.3. O acesso de representante da CONTRATADA nas dependências da CONTRATANTE, deverá ocorrer mediante prévia comunicação entre as partes, por meio dos mecanismos de comunicação definidos neste instrumento.
- 10.4. A entrega das subscrições e franquias (itens 4 e 5 do Lote I (WAAP)) se dará de forma virtual, via liberação do acesso na plataforma da solução.
- 10.5. A entrega dos serviços de treinamento (itens 3 e 6 do Lote I (WAAP) e item 2 do Lote II (ADC)) ocorrerá conforme as disposições do subtópico 15.2. (Requisitos de Capacitação) deste documento.

11. REGRAS PARA O RECEBIMENTO PROVISÓRIO E DEFINITIVO

- 11.1. O recebimento provisório do objeto, nos termos do art. 140, incisos I e II da Lei Federal nº 14.133/21 c/c o art. 20, I e II do Decreto nº 48.817/2023, será realizado pela Comissão de Fiscalização do Contrato da CONTRATANTE na forma abaixo indicada
- I - Para os bens de aquisição (itens 1 e 2 do Lote I - WAAP) e item 1 do Lote II - ADC)
 - a) de forma sumária, pelos fiscais dos contrato, após a entrega dos bens (appliance), com verificação posterior da conformidade do material com as exigências contratuais, nos termos do art. 140, II, a, da Lei Federal nº 14.133/2021 c/c o art. 20, II, a, do Decreto Estadual nº 44.817/2023.
 - II - Para os itens de serviço de subscrição/franquia (itens 4 e 5 do Lote I - WAAP)
 - a) pelos fiscais dos contratos, no prazo de 2 (dois) dias úteis, mediante termo, no prazo máximo de de 2 (dois) dias úteis a contar da entrega do Relatório de Cumprimento do Objeto;
 - III - Para os serviços de treinamento (itens 3 e 6 do Lote I -WAAP e item 2 do Lote II ADC)
 - a) pelos fiscais dos contrato, mediante termo, no prazo máximo de 2 (dois) dias úteis, a contar da entrega do Relatório de Cumprimento do Objeto.
 - IV - A CONTRATADA deverá elaborar um Relatório de Cumprimento do Objeto (modelo no Anexo II deste documento) a ser entregue à Comissão de Fiscalização de Contrato quando da entrega do bem ou serviço, para a análise antes da emissão do Termo de Recebimento Provisório. No caso dos itens de compra/aquisição (1 e 2 do Lote I - WAAP e item 1 do Lote II - ADC) o relatório não será entregue no recebimento sumário dos equipamentos, mas deverá ser entregue após a efetiva instalação e configuração dos mesmos para fins de emissão do Termo de Recebimento Definitivo deste itens. O relatório deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual (bens e serviços). O relatório deverá estar acompanhado, conforme item ou serviço entregue, das seguintes informações e/ou documentos:
 - a) Para os itens 1 e 2 do Lote I (WAAP) e item 1 do Lote II (ADC): entrega dos equipamentos adquiridos com a solução instalada e configurada; documentação que comprove o licenciamento desses equipamentos, tais como: número de série, chaves, dados para acionamento dos serviços de suporte e garantia, além dos documentos oficiais do fabricante e a documentação do produto (manuais, prospectos etc.);
 - b) Para o item 4 do Lote I (WAAP): evidências da disponibilização dos acessos aos usuários da Contratante e as evidências da implementação do escopo definido na Reunião de Kick Off.
 - c) Para o item 5 do Lote I (WAAP): relatório da ferramenta onde conste o consumo de throughput excedente;
 - d) Para os itens 3 e 6 do Lote I (WAAP) e item 2 do Lote II (ADC): certificados dos alunos treinados.
- 11.2. 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.
- 11.3. 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.
- 11.4. 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.
- 11.5. Estando em conformidade, será efetuado o recebimento definitivo.
- 11.6. O recebimento definitivo do objeto será efetuado pela Comissão de Fiscalização do Contrato, nos termos do art.140, incisos I e II da Lei Federal nº 14.133/2021, no prazo máximo de 20 (vinte) dias úteis, depois da emissão do Termo de Recebimento Provisório ou do recebimento sumário (no caso dos itens 1 e 2 do Lote I (WAAP) e item 1 do Lote II (ADC), após o que poderá ser verificada a conformidade das quantidades e especificações com aquelas contratadas e consignadas no Termo de Referência.
- 11.7. Com o recebimento definitivo, que concretiza o ateste do cumprimento do objeto (bens e serviços) contratado, a CONTRATANTE comunicará à CONTRATADA para que, em até 5 dias, emita a Nota Fiscal ou Fatura.
- 11.8. 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.
- 11.9. 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.
- 11.10. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens fornecidos (appliances) e os serviços de subscrições correlatos, nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pelo Decreto nº 48.817/2023 e pelo contrato a ser celebrado.

12. DEFINIÇÃO DAS CONDIÇÕES DOS SERVIÇOS DE MANUTENÇÃO, ASSISTÊNCIA TÉCNICA, SUPORTE E GARANTIA DO BEM/SERVIÇO

- 12.1. **Manutenção**
- 12.1.1. Todas as rotinas para fins de manutenção com vistas ao pleno e adequado funcionamento das soluções ao longo da vigência contratual estarão a cargo da CONTRATADA na forma do Suporte Técnico previsto nos subtópicos 12.2.1 e 12.2.2 deste documento. O referido Suporte Técnico contempla a manutenção corretiva com o objetivo solucionar defeitos encontrados no software, e também a manutenção evolutiva na forma da atualização oportuna das soluções contratadas.
- 12.1.2. O fornecedor deve disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.
- 12.2. **Suporte Técnico e garantia do produto**
- 12.2.1. Suporte técnico
- I - 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);
 - II - A contratante poderá efetuar um número ilimitado de chamados para suporte técnico, durante a vigência da garantia, para suprir suas necessidades com relação a solução adquirida;

III - Considera-se “suporte técnico” a facilidade de comunicação colocada à disposição do CONTRATANTE para a prestação de informações, esclarecimentos ou orientações sobre a utilização, funcionalidades (dicas e atalhos), configuração de softwares/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;

IV - O suporte técnico será acionado 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;

V - 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 do contratante decidirá sobre a aplicação ou não das recomendações;

VI - 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 suporte;

VII - CONTRATADA deverá assegurar que, em caso de constatação de falha física do hardware, um novo equipamento de mesmo product/part number ou superior compatível, deverá ser enviado em até 1 (um) dia útil para substituição imediata no ambiente da CONTRATANTE, sem ser necessário que a CONTRATANTE envie o equipamento defeituoso à CONTRATADA;

VIII - Os prazos de atendimento do suporte técnico da solução devem ter como referência os níveis de severidade, todos informados nas tabelas abaixo, ficando a contratada sujeita às sanções previstas na lei em caso de descumprimento contratual:

WAAP			
Severidade	Descrição	Tempo do Contrato 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

ADC			
Severidade	Descrição	Tempo do Contrato 1º contato após abertura do chamado	Tempo de solução
Alta	Objeto totalmente inoperante	até 30 minutos	até 2 horas
Média alta	Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 1 hora	até 4 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 2 horas	até 8 horas
Baixa	Solicitações de informações diversas ou dúvidas sobre a solução	até 4 horas	até 24 horas

IX - 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;

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

XI - 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;

XII - O serviço de suporte técnico deverá ser prestado em regime 24x7x365 (vinte e quatro horas por dia durante todos os dias do ano, inclusive sábados, domingos e feriados).

XIII - O suporte deverá ser preferencialmente realizado remotamente para solução de problemas, tratamento de falhas, dúvidas e orientações técnicas para a perfeita utilização da solução. Quando remotamente não for possível a resolução do chamado no prazo estabelecido, a continuidade do atendimento deverá ser de forma presencial, ou seja, com o especialista da CONTRATADA presente nas instalações da CONTRATANTE até o completo atendimento da demanda.

12.2.2. Suporte Técnico para os serviços Subscrição/franquia - WAAP

I - Durante todo o período da subscrição, a Contratada será responsável pelo suporte técnico da solução tecnológica que compõe a solução WAAP em nuvem (SaaS), composta pelos itens 4 e 5 do Lote I.

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

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

IV - 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).

V - Os chamados abertos por órgão contratante no sistema de chamados da Contratada não poderão ser visualizados por outros órgãos contratantes.

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

Severidade	Descrição	Tempo do 1º contato após abertura do chamado	Tempo de solução
Alta	Objeto totalmente inoperante	até 30 minutos	até 4 horas
Média alta	Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 1 hora	até 8 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 4 horas	até 16 horas
Baixa	Solicitações de informações diversas ou dúvidas sobre a solução	até 24 horas	até 72 hoas

VII - O suporte técnico deverá contemplar manutenção corretiva e evolutiva para a solução contratada, e não poderá acarretar custos adicionais ao Contratante.

VIII - Entende-se por manutenção corretiva uma série de procedimentos destinados a recolocar a solução em pleno estado de funcionamento, removendo definitivamente os defeitos apresentados.

IX - Entende-se por manutenção evolutiva o fornecimento de novas versões e/ ou releases corretivas e/ou evolutivas de softwares que compõem a solução, que venham a ser lançadas durante a vigência do contrato.

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

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

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

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

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

12.2.3. Garantia do Produto

12.2.4. A Garantia de produto para os bens de compra obedecerá às seguintes regras:

I - A garantia terá duração de 36 (trinta e seis) meses, contados a partir da data do recebimento definitivo do objeto;

II - Considera-se “garantia” a obrigação da CONTRATADA em reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, o objeto do contrato (e quaisquer de seus componentes) em que se verificarem vícios de produto, defeitos ou incorreções, durante o prazo de garantia especificado neste documento;

III - A garantia deve obrigatoriamente prover, ao longo de sua duração e sem ônus adicionais para o contratante, o seguinte:

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

b) Revisões dos manuais técnicos e/ou documentação dos equipamentos adquiridos.

13. METODOLOGIA DE AVALIAÇÃO DA QUALIDADE E ACEITE DO OBJETO EXECUTADO, E, QUANDO SE TRATAR DE SERVIÇOS E FOR APLICÁVEL, O ACORDO DE NÍVEL DE SERVIÇO – ANS

13.1. Metodologia de Avaliação da Qualidade e Aceite do Objeto Executado (ANS)

13.1.1. Acordo de Nível de Serviço

13.1.1.1. Para os serviços de subscrição/franquia

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

II - Periodicidade: Trimestral

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

IV - Mecanismo de cálculo: Na forma da tabela do subtópico 12.2.2, inciso VI, deste documento.

13.1.1.2. Para os serviços de treinamento

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

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

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

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

a) I (insatisfatório) – 0 a 25%;

b) R (regular) – 26 a 50%;

c) B (bom) – 51 a 75%;

d) MB (muito bom) – 76 a 100%.

13.1.2. Penalidades

13.1.2.1. Poderá ocorrer a aplicação de multas por motivo de descumprimento de nível de serviço exigido, conforme valores a seguir:

I - Para os serviços de subscrição/franquia:

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

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

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

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

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

II - Para os serviços de treinamento:

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

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

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

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

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

13.1.2.4. As multas por não cumprimento dos níveis de serviço serão descontadas da garantia de contrato prevista no subtópico 16 deste documento, resguardado o limite da mesma.

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

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

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

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

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

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

14. CRITÉRIOS DE MEDIÇÃO, DE PAGAMENTO, CONDIÇÕES DE AQUISIÇÃO E REAJUSTAMENTO DO CONTRATO

14.1. Pagamento

14.1.1. O CONTRATANTE deverá pagar o preço ao CONTRATADO, consideradas as formas previstas por item nas alíneas abaixo, na conta corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro:

- a) Para os bens de compra (itens 1 e 2 do Lote I (WAAP) e item 1 do Lote II (ADC)) em parcela única a ser efetuada à vista, após o recebimento definitivo do item.;
- b) Para os serviços de treinamento (itens 3 e 6 do Lote I (WAAP) e item 2 do Lote II (ADC)) e serviço de franquia de dados (item 5 do Lote I - WAAP) em parcelas sob demanda, após o recebimento definitivo do item.;
- c) Para os serviços de subscrição (item 4 do Lote I (WAAP)) em parcela única a ser efetuada à vista.

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

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

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

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

14.1.6. Uma vez recebido o documento mencionado no subtópico 14.1.5, o órgão competente deverá verificar:

- I - a manutenção das condições de habilitação exigidas pelo instrumento convocatório;
- II - por consulta, aos cadastros mencionados nas alíneas abaixo, se o contratado foi penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o poder público mediante consulta aos cadastros oficiais do poder público existentes, observadas as abrangências de aplicação:
 - a) SICAF;
 - b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/ceis>);
 - c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php);
 - d) Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (<https://www.portaltransparencia.gov.br/sancoes/cnep>);
 - e) Lista de inidôneos mantida pelo Tribunal de Contas da União; e
 - f) módulo Registro de Ocorrências do SIGA.
- III - por consulta ao SICAF, eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas apontadas ao Relatório de Ocorrências Impeditivas Indiretas.

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

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

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

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

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

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

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

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

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

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

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

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

14.2. **Reajuste de Preços**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15. **REQUISITOS DA CONTRATAÇÃO**

15.1. **Requisitos de Negócio**

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

15.1.1.1. Adicionar uma camada de proteção nas aplicações web hospedadas na infraestrutura do órgão ou entidade contratante, através da contratação de solução tecnológica que ofereça, as seguintes funcionalidades: Web Application Firewall, Proteção a APIs, Proteção contra DDoS, Mitigação de Bots, Gerenciamento e Proteção de DNS e Balanceamento de Carga, performance de aplicações e inspeção SSL.

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

15.1.1.3. A solução tecnológica utilizada na prestação dos serviços de subscrição de software e de franquia deverão estar disponíveis para acesso da CONTRATANTE por ao menos 99,5% do referido período contratual.

15.1.1.4. Garantia de 36 meses para todos os componentes de compra perpétua da solução, observados os seguintes aspectos:

a) A garantia para os itens de aquisição em modalidade perpétua, por período de 36 meses, costuma ser praxe em licitações para contratações de soluções de TIC, tanto pelo governo federal como pelos demais entes, em que pese significar um aspecto diferencial do produto que, por fugir da condição básica ofertada pelo fornecedor, decerto que interfere em sua precificação e poderá repercutir numa majoração do lance do licitante no momento do pregão.

b) Esta garantia visa resguardar o bom funcionamento do inventário de TIC, com soluções de software e hardware em boas condições de forma a preservar o desempenho e a produtividade dos órgãos que venham a contratar o objeto (bens e serviços) ora proposto.

c) Por fim, dentro da mesma lógica do legislador, ao autorizar o poder público para contratações iniciais por prazos de até 5 (cinco) anos (com potencial alcance de até 10 (dez) anos, naturalmente com o fim de resguardar a continuidade dos serviços públicos, que aliás, é um princípio da Administração Pública, é que se propõe a garantia de 36 meses para as soluções de TIC a serem adquiridas.

15.2. **Requisitos de Capacitação**

15.2.1. A capacitação compreende os serviços de treinamentos.

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

15.2.3. Deverá ser entregue para a contratante, na reunião kick off prevista neste documento, a proposta com o conteúdo do treinamento.

15.2.4. A Contratante reserva-se o direito de não aceitar o módulo ministrado, podendo, a seu critério, solicitar a troca de instrutor ou até mesmo repetição do mesmo, caso não seja satisfatório.

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

15.2.6. Deverá ser fornecido pela contratada certificado de capacitação para os participantes do treinamento.

15.2.7. **Objetivo**

15.2.7.1. Capacitação do contratante para a operacionalização da ferramenta tecnológica.

15.2.7.2. Formação de facilitadores que possam vir a replicar futuramente o conhecimento no âmbito do órgão contratante.

15.2.8. **Métrica**

O treinamento será contratado por turma de 8 alunos.

15.2.9. **Carga horária**

15.2.9.1. Deverá ter carga horária mínima de 40 (quarenta) horas.

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

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

15.2.10. **Forma de realização**

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

15.2.11. **Materiais didáticos e acessórios**

15.2.11.1. É de responsabilidade da contratada todo material audiovisual, didático e eletrônico para a realização dos treinamentos, e quaisquer outras despesas diretas ou

indiretas.

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

15.2.12. **Conteúdo programático**

15.2.12.1. 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.

15.2.12.2. O evento abordará 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.

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

15.3. **Requisitos Legais Aplicáveis ao Objeto:**

Sem previsão de normatização específica pertinente às soluções tecnológicas previstas no objeto.

15.4. **Requisitos Temporais**

15.4.1. Resguardado os cronogramas previstos no subtópico 9.2.2.1 deste documento, não há outros requisitos temporais a serem considerados.

15.5. **Endereço de Entrega**

Conforme o item 10 deste documento.

15.6. **Requisitos de Metodologia de Trabalho**

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

- a) Ordem de Serviço / Ordem de Fornecimento;
- b) Termos de Recebimento;
- c) Chamado registrado na Central de Atendimento;
- d) Ofícios;
- e) Relatórios e Atas de Reunião;
- f) E-mail;
- g) Demais Termos previstos no instrumento convocatório.

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

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

15.7. **Requisitos de Sustentabilidade Ambiental**

15.7.1. No que for aplicável, a contratada deverá promover a correta destinação dos resíduos resultantes da prestação do serviço, tais peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental (Lei nº 12.305/2010).

15.7.2. Deverá ainda obedecer aos critérios previstos no capítulo I do Decreto 43.629/2012, por meio dos artigos 1º e 2º, in verbis:

Art. 1º - As especificações para a aquisição de bens, contratação de serviços e obras por parte dos órgãos e entidades da Administração Pública Estadual Direta e Indireta, a fixação de critérios de julgamento e a execução e fiscalização dos respectivos contratos, observarão critérios de sustentabilidade ambiental, na forma deste Decreto.

Art. 2º - Consideram-se critérios de sustentabilidade ambiental, dentre outros:

- I- economia no consumo de água e energia;
- II- minimização da geração de resíduos e destinação final ambientalmente adequada dos que forem gerados;
- III- racionalização do uso de matérias-primas;
- IV- redução da emissão de poluentes;
- V- adoção de tecnologias menos agressivas ao meio ambiente;
- VI- implementação de medidas que reduzam as emissões de gases de efeito estufa e aumentem os sumidouros;
- VII- utilização de produtos de baixa toxicidade;
- VIII- utilização de produtos com a origem ambiental sustentável comprovada, quando existir certificação para o produto.

15.7.3. A contratada deverá, no que for aplicável ao cumprimento do objeto, obedecer aos demais critérios estabelecidos no Decreto Estadual nº 43.629/2012.

15.8. **Requisitos Culturais**

Não se aplicam requisitos culturais.

15.9. **De Arquitetura Tecnológica**

15.9.1. Os requisitos tecnológicos de arquitetura da solução, relacionados aos bens de compra e aos serviços de subscrição e franquia, constarão nos subtópicos 2.2, 2.3, 2.4, 2.5 e 3.2 do Anexo I - Especificações Técnicas do Objeto.

15.9.2. Os requisitos tecnológicos relacionados aos serviços de treinamento, encontram-se no subtópico 15.2. (Requisitos de Capacitação) deste documento.

15.9.3. Durante a reunião de kick-off (vide subtópico 15.10.1. deste documento), a CONTRATADA deverá apresentar a arquitetura das soluções (Plano de Execução) 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.

15.10. **Requisitos de Projeto e de Implementação**

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

15.10.2. Após a reunião de kick-off a CONTRATADA deverá produzir e entregar ao CONTRATANTE o Plano de Execução elaborado com base no quanto acertado ao longo da reunião, contemplando o planejamento, escopo, cronograma, discriminação dos produtos entregáveis, dimensionamento da infraestrutura tecnológica necessária, discriminação da equipe do projeto com perfis e quantitativos mínimos, relatório de controle e tratamento de riscos do projeto e demais artefatos que se façam necessários no entendimento da Contratante.

15.10.3. Compreende-se nesta etapa a instalação de equipamentos, sistemas, softwares e aplicativos da CONTRATANTE nos PRODUTOS fornecidos, bem como a migração das configurações existentes na CONTRATANTE para os produtos fornecidos pela CONTRATADA, caso haja viabilidade;

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

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

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

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

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

15.10.9. 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, tuning, resolução de problemas e implementação de segurança.

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

- a) Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares e recursos humanos necessários à instalação das soluções;
- b) Caberá à CONTRATADA disponibilização de ferramentas / scripts de retorno imediato ao estado original da estrutura da CONTRATANTE caso a instalação dos produtos / softwares da CONTRATADA apresente falha.
- c) 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.

15.10.11. O fornecedor deverá submeter previamente, por escrito, à Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações acordadas.

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

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

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

15.11.2. A equipe a ser disponibilizada pelo fornecedor para fins de contratação e prestação de todos os serviços, deverá comprovadamente ser qualificada e com experiência na atividade objeto da contratação.

15.12. **Requisitos Materiais e Humanos**

15.12.1. Materiais, insumos e acessórios necessários ao perfeito funcionamento das soluções fornecidas deverão ser arcados pela CONTRATADA, sem custos adicionais para a CONTRATANTE.

15.12.2. 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.

15.12.3. Em observação ao entendimento do Enunciado nº 14, item 5 da Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ, saliente-se que o objeto da presente contratação, que contempla serviços de treinamento e subscrição de solução tecnológica, não prevê o uso de mão de obra residente/dedicada nas dependências do órgão contratante. Adicionalmente registre-se que o objeto também não caracteriza, forma alguma, terceirização de atividade-fim, tendo em vista que se trata de contratação, em regime de compra de equipamentos de tecnologia e respectivos cursos de treinamento, bem como suporte técnico específico do fabricante/fornecedor representante, no âmbito da garantia comum de mercado, que estão diretamente relacionado à atuação de profissionais e especialistas nas soluções contratadas.

15.13. **Necessidades de Adequações no Ambiente**

Não há previsão de ações antecedentes ao contrato se façam necessárias por parte do CONTRATANTE.

15.14. **Reunião de kick-off**

Vide subitem 15.10 deste documento.

16. **PREVISÃO E CONDIÇÕES DE PRESTAÇÃO DA GARANTIA CONTRATUAL**

16.1. O Contrato conta com garantia de execução, nos moldes do artigo 96 da Lei nº 14.133/2021, correspondente a:

- a) 5% (cinco por cento) do valor inicial atualizado do contrato, para os itens 1 e 2 do Lote I e item 1 do Lote II;
- b) 5% (cinco por cento) do valor anual do contrato, para os itens 4 e 5 do Lote I;
- c) 5% (cinco por cento) do valor inicial atualizado do contrato, para os itens 3 e 6 do Lote I e item 2 do Lote II.

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

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

- a) caução em dinheiro ou em títulos da dívida pública;
- b) seguro-garantia; e
- c) fiança bancária.
- d) título de capitalização custeado por pagamento único, com resgate pelo valor total.

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

- a) prejuízos advindos do não cumprimento do objeto do Contrato e do não adimplemento das demais obrigações neste previstas;
- b) multas moratórias, compensatórias e administrativas aplicadas pela Administração ao CONTRATADO; e
- c) obrigações trabalhistas e previdenciárias de qualquer natureza, assim como as obrigações de regularidade perante o FGTS, não adimplidas pelo CONTRATADO, quando couber.

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

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

16.7. Ressalvada a hipótese de seguro-garantia, em que deverá ser observado o prazo do item 16.8, o CONTRATADO apresentará, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do CONTRATANTE, contado da assinatura do Contrato, o comprovante de prestação de garantia, na forma do item 16.3.

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

- a) a apólice permanecerá em vigor mesmo que o CONTRATADO não pague o prêmio nas datas convencionadas;
- b) a apólice deverá acompanhar as modificações referentes à vigência do Contrato principal, mediante a emissão do respectivo endosso pela seguradora;
- c) será permitida a substituição da apólice na data de renovação ou de aniversário, desde que mantidas as condições e coberturas da apólice vigente e nenhum período fique descoberto, ressalvado o disposto no item 16.6; e
- d) a apólice somente será aceita se contemplar todos os eventos indicados no item 16.4, observada a legislação que rege a matéria.

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

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

16.11. Caso a opção seja por garantia em dinheiro, deverá ser efetuada em favor do CONTRATANTE, na conta-corrente da instituição financeira contratada pelo Estado, cujo valor será corrigido monetariamente e restituído ao CONTRATADO, na forma do item 16.9.

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

exija a manutenção da condição disposta no subitem 16.1.

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

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

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

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

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

16.18. Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

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

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

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

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

17. INDICAÇÃO DE MARCAS E MODELOS OU VEDAÇÃO DE UTILIZAÇÃO DE MARCA/PRODUTO NA EXECUÇÃO DO SERVIÇO

17.1. Não há preferência por marcas ou modelos específicos. Todas as propostas serão analisadas de acordo com as especificações técnicas e critérios de desempenho estabelecidos, garantindo a competitividade e imparcialidade no processo de seleção.

18. MODELO DE GESTÃO DO CONTRATO

18.1. Na forma do art. 4º do Decreto estadual nº 48.817/2023, a gestão e a fiscalização da execução da contratação serão realizadas por agentes públicos, designados pela autoridade do órgão ou entidade contratante, que indicará o gestor e fiscais para cada contrato, dentre os servidores lotados no órgão ou entidade, bem como seus substitutos, observando-se os requisitos estabelecidos na Lei nº 14.133/2021.

18.2. A gestão e a fiscalização da execução da contratação poderá ser realizada por uma Comissão de Gestão e Fiscalização, composta por, no mínimo, 3 (três) membros, integrada por gestor, fiscais e complementada conforme a necessidade pelos agentes definidos nos incisos I a III do art. 5º do Decreto acima referido, considerando a especificidade e complexidade do objeto ou da solução, de acordo com a necessidade e a critério da administração.

18.3. A Comissão de Gestão e Fiscalização anotará, em registro próprio, todas as ocorrências relacionadas com a execução do contrato, determinando o que for necessário à regularização das faltas ou defeitos observados.

18.4. A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, definidos no art. 18 do Decreto estadual nº 48.817/2023.

18.5. Deve ser estabelecido, desde o início da execução contratual, mecanismo de controle da utilização dos materiais empregados nos contratos, para efeito de acompanhamento da execução do objeto bem como para subsidiar a estimativa para as futuras contratações.

18.6. O contratado declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que esta necessitar e que forem julgados necessários ao desempenho de suas atividades.

18.7. A instituição e a atuação da fiscalização não exclui ou atenua a responsabilidade do contratado, nem a exime de manter fiscalização própria.

18.8. É vedada a atribuição ao contratado da avaliação de desempenho e qualidade da prestação dos serviços por ela realizada.

19. EXIGÊNCIAS DE HABILITAÇÃO JURÍDICA, TÉCNICA, FISCAL, SOCIAL E TRABALHISTA E ECONÔMICO-FINANCEIRA

19.1. Habilitação Jurídica

19.1.1. Pessoa física: cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional.

19.1.2. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede.

19.1.3. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br.

19.1.4. Sociedade Limitada Unipessoal - SLU: ato constitutivo, estatuto ou contrato social em vigor inscrito no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhado de documento comprobatório do administrador, sendo assim enquadrada a sociedade identificada como Empresas Individual de Responsabilidade Limitada – EIRELI, na forma do art. 41, da Lei nº 14.195, de 26 de agosto de 2021.

19.1.5. Sociedade Empresária Estrangeira em funcionamento no País: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020 ou norma posterior que regule a matéria.

19.1.6. Sociedade Simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores.

19.1.7. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde se encontra estabelecida a matriz.

19.1.8. Quando cabível, os documentos apresentados devem estar acompanhados de todas as alterações ou da consolidação respectiva.

19.2. Habilitação Técnica

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

19.2.2. O(s) atestado(s) deverão demonstrar o cumprimento de um quantitativo mínimo de 30% (trinta por cento) do volume estimado para cada um dos itens: 1, 2 e 4 do Lote I (WAAP) e para o item 1 do Lote II (ADC), os quais correspondem às respectivas parcelas de maior relevância ou de valor significativo para o objeto deste certame.

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

19.2.4. Os atestados deverão referir-se a fornecimento/serviço prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

19.2.5. Será admitida, para fins de comprovação de quantitativo mínimo do fornecimento/serviço, a apresentação de diferentes atestados de objetos executados de forma concomitante, resultando na comprovação de capacidade técnico operacional de uma única contratação.

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

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

19.3. **Habilitação fiscal, Social e Trabalhista**

19.3.1. Inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso.

19.3.2. Regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social.

19.3.3. Regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS).

19.3.4. Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do art. 7º, XXXIII, da Constituição.

19.3.5. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

19.3.6. Prova de inscrição no cadastro de contribuintes estadual/distrital e municipal, relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual

19.3.7. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123/2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal, eis que a apresentação do Certificado de Condição de Microempreendedor Individual – CCMEI supre tais requisitos.

19.3.8. Prova de regularidade com a Fazenda do Estado do Rio de Janeiro, mediante a apresentação de:

a) Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, expedida pela Secretaria de Estado de Fazenda;

b) Certidão Negativa de Débitos em Dívida Ativa, ou Certidão Positiva com efeito de Negativa, para fins de participação em licitação, expedida pela Procuradoria Geral do Estado.

19.3.9. (para os itens de serviço previstos no objeto) Regularidade com a Fazenda Municipal do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre, com a apresentação de Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, do imposto sobre serviços de qualquer natureza – ISS.

19.3.10. (para os itens de compra previstos no objeto) Regularidade com a Fazenda Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre, com a apresentação de Certidão Negativa de Débitos, ou Certidão Positiva com efeito de Negativa, perante o Fisco estadual, pertinente ao Imposto sobre Operações relativas à Circulação de Mercadorias e sobre Prestações de Serviços de Transporte Interestadual, Intermunicipal e de Comunicação – ICMS, bem como de Certidão perante a Dívida Ativa estadual, podendo ser apresentada Certidão Conjunta em que constem ambas as informações.

19.3.11. Caso o fornecedor seja considerado isento dos tributos municipais/estaduais relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

19.3.12. Na hipótese de cuidar-se de microempresa ou de empresa de pequeno porte, na forma do art. 42 da Lei Complementar nº 123/2006, a documentação somente será exigida para efeito de assinatura do contrato, caso se sagre vencedora no certame.

19.3.13. Em sendo declarada vencedora do certame microempresa ou empresa de pequeno porte com débitos fiscais e trabalhistas, ficará assegurado, a partir de então, o prazo de 5 (cinco) dias úteis para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de negativas, na forma do art. 43, § 1º, da Lei Complementar nº 123/2006.

19.3.14. O prazo acima poderá ser prorrogado por igual período, a critério exclusivo da Administração Pública.

19.3.15. A não regularização da documentação no prazo estipulado implicará a decadência do direito à contratação, na forma do § 2º do art. 43 da Lei Complementar nº 123/2006, sem prejuízo de aplicação de sanções previstas no Edital.

19.4. **Habilitação Econômico-Financeira**

19.4.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor, caso se trate de pessoa jurídica, ou certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do fornecedor, caso se trate de pessoa física ou de sociedade simples.

19.4.2. Não será causa de inabilitação do licitante a anotação de distribuição de processo de recuperação judicial ou de pedido de homologação de recuperação extrajudicial.

19.4.3. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, vedada a sua substituição por balancetes ou balanços provisórios.

19.4.4. Os documentos referidos acima limitar-se-ão ao último exercício social no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

19.4.5. Os fornecedores criados no exercício financeiro da contratação deverão atender a todas as exigências da habilitação e ficam autorizados a substituir os demonstrativos contábeis pelo balanço de abertura;

19.4.6. Poderá ser apresentado o balanço intermediário, caso autorizado por lei ou pelo contrato/estatuto social.

19.4.7. Para fins de habilitação econômico-financeira de sociedade empresária em recuperação judicial deverão ser considerados os valores constantes no Plano de Recuperação Judicial, homologado pelo Juízo competente, para fins de apuração dos índices contábeis previstos no edital.

19.4.8. Comprovação da boa situação financeira da empresa mediante obtenção de índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), iguais ou superiores a 1 (um), obtidos pela aplicação das seguintes fórmulas:

$$LG = \frac{\text{Ativo Circulante} + \text{Realizável a Longo Prazo}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante} + \text{Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

19.4.9. Caso seja apresentado resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverá ser comprovado capital ou patrimônio líquido mínimo de 1% (um por cento) do valor total estimado da contratação ou do item pertinente.

19.4.10. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

19.4.11. As exigências de habilitação econômico-financeira descritas no subitem 19.4 tem como objetivo assegurar que o licitante tenha condições de cumprir as obrigações contratuais, garantindo a qualidade e a execução do contrato.

19.4.12. Ao verificar a saúde financeira do licitante, a administração pública reduz o risco de inadimplência, atrasos e problemas na execução do contrato.

19.4.13. A apresentação do balanço patrimonial e das demonstrações contábeis contribui para a transparência do processo licitatório, permitindo que a administração pública avalie a situação financeira do licitante de forma mais precisa.

20. **OBRIGAÇÕES DA CONTRATANTE E CONTRATADA**

20.1. **OBRIGAÇÕES DA CONTRATANTE:**

- a) Fornecer à CONTRATADA documentos, informações e demais elementos que possuir pertinentes à execução do objeto;
- b) Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- c) Encaminhar formalmente a demanda por meio de Autorização de Fornecimento, de acordo com os critérios estabelecidos neste Termo de Referência.

20.2. **OBRIGAÇÕES DA CONTRATADA:**

- a) 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;
- b) Entregar o objeto acompanhado, se for o caso, do manual do usuário, com uma versão em português, e da relação da rede de assistência técnica autorizada;
- c) Comunicar à CONTRATANTE, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;
- d) Indicar formalmente preposto apto a representá-lo junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;
- e) Assinar o Termo de Confidencialidade e Sigilo, conforme o modelo apresentado no Anexo III deste documento;
- f) Disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas.
- g) 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.
- h) Caso o valor do Contrato se enquadre no limite previsto no art. 1º da Lei estadual nº 7.753, de 17 de outubro de 2017, manter Programa de Integridade nos termos da referida Lei e eventuais modificações e regulamentos subsequentes, consistindo tal programa no conjunto de mecanismos e procedimentos internos de integridade, auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com o objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a Administração Pública;
- i) Caso o fornecedor registrado ainda não tenha programa de integridade instituído, deverá implantar o Programa de Integridade no prazo de até 180 (cento e oitenta) dias corridos, a partir da assinatura do Contrato, na forma da legislação vigente.

20.3. **OBRIGAÇÕES PERTINENTES À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)**

I - Definições Gerais:

As partes (CONTRATANTE e CONTRATADO) deverão cumprir a (Lei Geral de Proteção de Dados - LGPD), e o Decreto Estadual nº 48.891/2024 (Institui a Política de Governança Em Privacidade e Proteção de Dados Pessoais do Estado do Rio de Janeiro), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa, conforme manifestação destes autos (112363412).

Para os fins da LGPD, na forma do seu art. 5º, incisos VI e VII, a CONTRATANTE corresponderá ao CONTROLADOR, enquanto a CONTRATADO corresponderá ao OPERADOR.

II - Obrigações Gerais das Partes:

As partes deverão adotar, em relação aos dados pessoais, medidas de segurança, técnicas e administrativas, aptas a proteger os dados e informações de acessos, não autorizados, e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, ou ilícito.

O CONTRATADO deve notificar imediatamente, à CONTRATANTE, a ocorrência de incidente de segurança, relacionado a dados pessoais, por ela tratados, fornecendo informações suficientes para que a CONTRATANTE cumpra quaisquer obrigações de comunicação da ocorrência, à autoridade nacional, e aos titulares dos dados.

III - Obrigações Específicas das Partes:

As partes deverão, nomeadamente:

- a - tratar os dados pessoais nos moldes expressamente definidos e em estrita consonância com a finalidade específica delineada pelo CONTROLADOR;
- b - armazenar os dados pessoais apenas durante o período definido pelo CONTROLADOR;
- c - não desviar o tratamento dos dados pessoais da finalidade específica e da hipótese legal legitimadora;
- d - informar imediatamente a outra parte contratante acerca da ocorrência de qualquer incidente que envolva os dados pessoais tratados, assim como prestar toda colaboração necessária para instruir o respectivo Relatório;
- e - assegurar os direitos dos titulares, abrangendo a disponibilidade de canal acessível ao Encarregado Setorial pelo tratamento de dados pessoais;
- f - garantir que os respectivos colaboradores ou prestadores de serviços que tenham acesso aos dados pessoais no contexto do Termo de Referência cumpram as diretrizes protetivas dos dados pessoais, vinculando-os a um Termo de Confidencialidade.

As partes, no âmbito de suas competências, deverão estabelecer regras de boas práticas e de governança que estabeleçam os aspectos procedimentais adequados para o cumprimento das diretrizes normativas, como:

- a - as condições de organização;
- b - o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares;
- c - as normas de segurança;
- d - os padrões técnicos;
- e - as obrigações específicas para os diversos envolvidos no tratamento;
- f - as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos.

IV - Responsabilidades e Restrições:

A responsabilidade pelo cumprimento das diretrizes contempladas na Lei Federal nº 13.709/2018, especialmente no tocante ao tratamento de dados pessoais adequados e legítimos, será de responsabilidade do órgão contratante que, ao figurar como agente de tratamento, assumirá as obrigações imputadas na legislação.

Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

É vedada a transferência de dados pessoais, pela CONTRATADO, para fora do território do Brasil sem o prévio consentimento, por escrito, do CONTRATANTE, e demonstração da observância, pela CONTRATADO, da adequada proteção desses dados, cabendo ao CONTRATADO o cumprimento de toda a legislação de proteção de dados ou de privacidade de outro (s) país (es) que for aplicável.

V - Subcontratação:

Não será admitida a subcontratação, sub-rogação, cessão ou transferência no todo ou em parte, em razão da composição do objeto, distribuído em lotes compostos por itens de softwares a serem contratados sob forma de aquisição perpétua ou sob forma de subscrição/licença temporária, juntamente com os respectivos cursos de capacitação, não se aplicando a divisão do objeto conforme previsto no item 20 do Estudo Técnico Preliminar - ETP.

VI - Término do Tratamento:

Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do CONTRATADO eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

VII - Tratamento Automatizado de Dados Pessoais:

Caso o tratamento de dados pessoais realizado pelo CONTRATADO envolva decisões baseadas em processos automatizados, algoritmos, ou quaisquer soluções tecnológicas que produzam efeitos legais ou afetem de maneira relevante os interesses dos titulares dos dados, fica assegurado ao titular dos dados o direito de solicitar a revisão da decisão por pessoa natural, nos termos do art. 20 da LGPD.

O CONTRATADO deverá informar de maneira clara e adequada à CONTRATANTE sobre a existência de procedimentos automatizados nas operações de tratamento de dados e garantir mecanismos para atendimento aos pedidos de revisão realizados pelos titulares, conforme orientação do CONTROLADOR e exigências da Autoridade Nacional de Proteção de Dados (ANPD).

O CONTRATADO se compromete a não utilizar decisões automatizadas de forma indiscriminada, devendo sempre observar a boa-fé, transparência, adequação e necessidade quanto aos procedimentos estabelecidos, além de fornecer explicações claras sobre os critérios e parâmetros adotados nos sistemas automatizados, sempre que solicitado pelo CONTROLADOR ou pela autoridade competente.

VIII - Treinamento, Fiscalização e Prestação de Informações:

É dever do CONTRATADO orientar, treinar e exigir que seus colaboradores envolvidos no tratamento de dados pessoais e na execução dos serviços assinem um Termo de Confidencialidade e Sigilo sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

O CONTRATANTE poderá realizar diligência para aferir o cumprimento das obrigações pertinentes à LGPD, devendo o CONTRATADO atender prontamente eventuais pedidos de comprovação formulados, e deverá prestar, no prazo fixado pelo CONTRATANTE, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado nos moldes da LGPD.

IX - Gestão de Bancos de Dados e Políticas de Segurança:

Bancos de dados estruturados e não estruturados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização e portabilidade desses dados pela Administração nas hipóteses previstas na LGPD.

O CONTRATADO deve atender à Política de Segurança da Informação instituída pela Instrução Normativa PRODERJ PRE nº 07, de 25 de maio de 2025, e demais normativos correlatos publicados pelo CONTRATANTE.

X - Disposições Finais:

O Contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a Autoridade Nacional de Proteção de Dados (ANPD) por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

O CONTRATADO poderá responder por quaisquer danos, perdas ou prejuízos causados a CONTRATANTE, ou a terceiros, decorrentes do descumprimento da Lei Federal nº 13.709/2018 (LGPD), não excluindo ou reduzindo dessa responsabilidade a fiscalização do CONTRATANTE em seu acompanhamento

XI - Conclusão:

O uso de tecnologias deve estar alinhado com as finalidades institucionais dos órgãos e entidades, em conformidade com o princípio da necessidade previsto na Lei Geral de Proteção de Dados Pessoais (LGPD), conforme dispõe o art. 6º, inciso III:

“ III - Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.”

Com base nessas diretrizes, o Decreto Estadual nº 48.891/2024 estabelece no art. 8º os requisitos fundamentais para o tratamento de dados pessoais, reforçando a importância do consentimento e da clareza nas relações entre o controlador e o titular dos dados:

“A base legal adotada para o tratamento de dados pessoais pela Administração Pública Estadual deve ser definida de acordo com as finalidades do tratamento à luz do caso concreto, respeitados, em todos os casos, os direitos do titular de dados, os fundamentos e os princípios que informam a LGPD.”

Cabe destacar que além das competências previstas na LGPD deve-se também ser observado a Política de Governança em Privacidade e Proteção de Dados (Decreto Estadual nº 48.891/2024) e o Regulamento o Sistema de Registro de Preços (Decreto Estadual nº 48.843/2023).

Fica incumbido ao CONTRATANTE manter o Registro das Operações de Tratamento de Dados Pessoais, previsto no art. 37 da LGPD, o qual poderá ser solicitado pela Autoridade Nacional de Proteção de Dados (ANPD) para fins de fiscalização. Ademais, nos casos em que houver risco elevado às liberdades civis e aos direitos fundamentais dos titulares de dados, a ANPD poderá requerer do CONTRATANTE a elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), conforme estabelece o art. 38 da LGPD.

Dessa forma, os documentos mencionados contêm os elementos essenciais que conferem respaldo legal e técnico ao objeto tratado, não havendo, portanto, impedimentos para o regular prosseguimento do processo.

20.4. Demais obrigações serão definidas no contrato e no edital.

21. PREVISÃO DE PERCENTUAL MÍNIMO DE MÃO DE OBRA RESPONSÁVEL PELA EXECUÇÃO DO OBJETO DA CONTRATAÇÃO CONSTITUÍDO POR MULHERES VÍTIMAS DE VIOLÊNCIA DOMÉSTICA

21.1. Em razão das características do objeto, não haverá contratação de mão de obra para a sua execução pelo que se entende não ser aplicável o disposto no art. 17, V, "f" do Decreto Estadual nº 48.816/2023 à execução destes serviços, o que não exime a empresa CONTRATADA de cumprir a reserva de cotas de que dispõe a Lei Estadual nº 7.382/2016, quando cabível.

22. MODALIDADE DE LICITAÇÃO, CRITÉRIO DE JULGAMENTO E MODO DE DISPUTA

- 22.1. O fornecedor será selecionado por meio da realização de procedimento licitatório, na modalidade PREGÃO, sob a forma ELETRÔNICA, com a adoção do critério de julgamento pelo MENOR PREÇO por LOTE.
- 22.2. O modo de disputa será o ABERTO.
- 22.3. Em consonância ao inciso I do art. 56 da Lei Federal nº 14.133, de 2021 e atendimento ao art. 17, VI, "a" do Decreto Estadual nº 48.816/2023, no modo de disputa aberto, os licitantes apresentarão suas propostas por meio de lances públicos e sucessivos, crescentes ou decrescentes, visto que se trata de um pregão cujo critério de julgamento é menor preço por lote.
- 22.4. Os preços em disputa aberta ficam claros para melhor competição entre os participantes. Então, evitar riscos na contratação contribui para ter uma licitação que alcance mais prontamente os resultados pretendidos.
- 22.5. Outrossim, não foi possível identificar que optar por modo disputa diferente do "modo aberto" venha a trazer vantagem para a Administração e nem mesmo aponta simplificação do processo ou celeridade no resultado da licitação.

23. PREVISÃO DA VEDAÇÃO OU DA PARTICIPAÇÃO DE EMPRESAS SOB A FORMA DE CONSÓRCIO NO PROCESSO DE CONTRATAÇÃO E JUSTIFICATIVA PARA O CASO DE VEDAÇÃO

- 23.1. É vedada a participação de pessoas jurídicas reunidas em consórcio.
- 23.2. A vedação se dá em razão das características específicas da solução a ser contratada, que não pressupõe multiplicidade ou heterogeneidade de atividades empresariais distintas, nem envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital.
- 23.3. 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.
- 23.4. Ademais, a gestão compartilhada poderá gerar vícios ou lacunas no fluxo dos processos de atendimento. A cadeia de responsabilidades entre as empresas será maior que se o objeto estiver sob responsabilidade de uma única empresa, ainda que operacionalizado por meio de atuação conjunta com outras empresas.
- 23.5. Mesmo a garantia produzida como consequência da aquisição é resultado de equipes, técnicas e procedimento complementar, não havendo benefício ou necessidade de segmentação para a realização do objeto proposto, além de repercutir em vários canais de atendimento de eventuais chamados técnicos, gerando uma morosidade no atendimento e ocasionando o não cumprimento dos itens expostos no edital.
- 23.6. A ausência de consórcio não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.
- 23.7. Tendo em vista que é prerrogativa do Poder Público, na condição de CONTRATANTE, a escolha da participação ou não de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme a literalidade do texto da Lei nº 14.133/2021, art 15 e seus incisos e parágrafos, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.
- 23.8. Por fim, a vedação da participação de empresas reunidas em regime de consórcio visa exatamente afastar a restrição à competição, na medida em que a reunião de empresas que, individualmente, poderiam fornecer os equipamentos, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluíus/cartéis para manipular os preços nas licitações.

24. PREVISÃO DA VEDAÇÃO OU DA PARTICIPAÇÃO DE COOPERATIVA NO PROCESSO DE CONTRATAÇÃO E JUSTIFICATIVA PARA O CASO DE VEDAÇÃO

- 24.1. Não se faz razoável a participação de cooperativa de trabalho, qualquer que seja a sua forma de constituição, já que o objeto principal trata de compra de bens de aquisição perpétua (1 e 2 do Lote I (WAAP) e item 1 do Lote II (ADC)) e licenciamento temporário (subscrição) de software (itens 4 e 5 do Lote I (WAAP)). Ademais, no caso dos itens secundários de treinamento, há vínculo de subordinação direta entre o empregado e a empresa contratada para a prestação dos serviços.

25. PREVISÃO DA VEDAÇÃO OU DA POSSIBILIDADE DE SUBCONTRATAÇÃO, DO PERCENTUAL E DAS CONDIÇÕES

- 25.1. Não será admitida a subcontratação, sub-rogação, cessão ou transferência no todo ou em parte, em razão da composição do objeto, distribuído em lotes compostos por itens de softwares a serem contratados sob forma de aquisição perpétua (1 e 2 do Lote I (WAAP) e item 1 do Lote II (ADC)) ou sob forma de subscrição/licença temporária (itens 4 e 5 do Lote I (WAAP)), juntamente com os respectivos cursos de capacitação, não se aplicando a divisão do objeto.
- 25.2. Saliente-se que, no caso do item de treinamento ser ministrado pelo mesmo fabricante da solução ofertada pela contratada ou com uso de sua plataforma, isso não configura subcontratação, sub-rogação, cessão ou transferência, uma vez que compõe a solução.
- 25.3. Também não se configura subcontratação o acordo de representação, revenda e uso de solução tecnológica de terceiros.

26. ESTABELECIMENTO DE RESERVA DE COTA OU A EXCLUSIVIDADE DA LICITAÇÃO

- 26.1. Não se aplica, tendo em vista que o objeto desta licitação é distribuídos em dois lotes indivisíveis, os quais não podem, cada um, ser licitado separadamente, sem prejuízo do resultado ou da qualidade do objeto a ser futuramente contratado.
- 26.2. Ademais, os dois lotes previstos apresentaram nos estudo técnicos realizados, cada um, valor estimado superior ao teto informado no art. 48, I da Lei Complementar nº 123/2006.

27. PRAZO DE VALIDADE E CONDIÇÕES DA PROPOSTA

27.1. Condições da proposta

- 27.1.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:
- I - Valor unitário e total do item;
 - II - Marca;
 - III - Fabricante;
- 27.1.2. Descrição do objeto, contendo as informações similares à especificação deste Termo de Referência;
- 27.1.3. Quantidade cotada, que não poderá ser inferior ao quantitativo máximo de cada item que poderá ser adquirido.
- 27.1.4. Todas as especificações do objeto contidas na proposta vinculam o licitante.
- 27.1.5. O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.
- 27.1.6. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.
- 27.1.7. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.
- 27.1.8. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.
- 27.1.9. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.
- 27.1.10. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional, conforme §1º do art. 17 da Lei Complementar 123/2006.
- 27.1.11. O licitante cujo estabelecimento esteja localizado no Estado do Rio de Janeiro deverá apresentar proposta isenta de ICMS, quando cabível, de acordo com o Convênio CONFAZ nº 26/2003 e a Resolução SEFAZ nº 971/2016, sendo este valor considerado para efeito de competição na licitação.
- 27.1.12. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe este Termo de

Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

27.2. Prazo de Validade

27.2.1. O prazo de validade da proposta não será inferior a 60 (sessenta) dias corridos, a contar da data de sua apresentação, podendo ser prorrogado, por igual período, salvo se houver justificativa para prazo diverso aceita pela Administração.

27.2.2. Os licitantes devem respeitar os preços máximos estabelecidos no Anexo do Edital referente ao orçamento estimado (art. 59, III, da Lei nº 14.133/2021).

27.2.3. Os licitantes devem respeitar os preços unitários máximos estabelecidos no Anexo do Edital para os itens que compõem o lote, se for o caso.

27.2.4. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas do Estado e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

28. REGRAS PARA INSPEÇÃO DE AMOSTRA, POC OU PROVA DE CONCEITO

28.1. Conforme definido no estudo preliminar, não se faz necessária ao objeto, a aplicação de amostra ou protótipo, exame de conformidade, teste de bancada ou prova de conceito.

29. CRITÉRIOS DE DESEMPATE COM BASE NO DESENVOLVIMENTO PELO LICITANTE DE AÇÕES DE EQUIDADE ENTRE HOMENS E MULHERES NO AMBIENTE DE TRABALHO

29.1. O desenvolvimento, pelo licitante, de ações de equidade entre mulheres e homens no ambiente de trabalho será critério de desempate no processo licitatório, conforme disposto no art. 60, inciso III da Lei nº 14.133/2021, o art. 30 do Decreto nº 48.778/2023 e o art. 10 do Decreto nº 49.233/2024 que regulamentou a matéria no âmbito estadual.

29.2. Na forma disposta no art. 10, § 1º do referido normativo estadual, serão consideradas ações de equidade, respeitada a seguinte ordem:

I - medidas de recrutamento igualitário entre mulheres e homens;

II - igualdade de remuneração e paridade salarial entre mulheres e homens;

III - plano de carreira desenvolvido com expressa menção à ascensão profissional igualitária entre mulheres e homens, inclusive previsão de participação proporcional no quadro diretor da empresa;

IV - estabelecimento de canal de denúncia e garantia de apuração de práticas de assédio moral e sexual, inclusive com a implementação de políticas de tolerância zero com relação a todas as formas de violência no trabalho, incluindo abuso verbal e/ou físico;

V - ações em saúde e segurança do trabalho que considerem as diferenças entre os gêneros;

VI - investimentos na capacitação de mulheres para o exercício gerencial;

VII - promoção de programas educativos de gerentes e chefes de setores que possibilitem o reconhecimento de sinais de violência no ambiente de trabalho;

VIII - provisão de sala de apoio à amamentação com vistas a uma cultura de respeito e apoio à amamentação como forma de promover a saúde da mulher trabalhadora e de seu bebê, no caso de empresas que possuam em seus quadros mais de 30 (trinta) mulheres com idade superior a 16 (dezesesseis) anos, quantitativo previsto no art. 389, § 1º, do Decreto-Lei nº 5.452/1943 (Consolidação das Leis do Trabalho), de acordo com a estratégia "Apoio à Mulher Trabalhadora que Amamenta" do Ministério da Saúde e da Secretaria de Estado de Saúde; e

IX - adesão ao "Programa Empresa Cidadã", instituído pela Lei nº 11.770/2008, regulamentado pelos arts. 137 a 142 do Decreto nº 10.854/2021, destinados à prorrogação das licenças-maternidade e paternidade, mediante incentivo fiscal.

29.3. O licitante que atender, a pelo menos 2 (dois) dos incisos do § 1º do art. 10 (acima transcrito), terá sua proposta enquadrada no art. 60, inciso III da Lei nº 14.133/2021, para efeito de desempate, observado o disposto no § 5º do art. 42 do Decreto nº 48.778/2023.

29.4. O licitante que possuir o selo Empresa Amiga da Mulher, conferido nos termos da Lei nº 9.173/2021 e da Lei nº 14.682/2023 ou o selo Empresa Amiga da Amamentação, conferido pela Lei nº 14.683/2023 ficará dispensado da comprovação do desenvolvimento das ações de equidade de que trata o § 1º do art. 10 do Decreto estadual nº 49.233/2024.

30. CRITÉRIOS DE DESEMPATE COM BASE NO ART. 60 DA LEI Nº 14.133/2021

30.1. Em caso de eventual empate entre propostas ou lances, serão utilizados os seguintes critérios de desempate, nesta ordem, conforme regulamentação do Decreto estadual nº 48.778/2023:

I - contratação de microempresas e empresas de pequeno porte, nos termos dos arts. 44 e 45 da Lei Complementar nº 123/2006, observado o disposto no art. 4º da Lei nº 14.133/2021;

II - disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

III - avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei;

IV - desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme Decreto nº 49.233/2024;

V - desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

30.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

a) empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

b) empresas brasileiras;

c) empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

d) empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

31. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

31.1. O custo preliminar da contratação do Lote I, estimado na fase do Estudo Técnico é de **RS 7.136.208,72 (sete milhões, cento e trinta e seis mil, duzentos e oito reais e setenta e dois centavos)**.

31.2. O custo preliminar da contratação do Lote II, estimado na fase do Estudo Técnico é de **RS 8.198.074,52 (oito milhões, cento e noventa e oito mil, setenta e quatro reais e cinquenta e dois centavos)**.

31.3. A estimativa do valor da contratação elaborada com base nos requisitos dos arts. 28 a 32 do Decreto estadual nº 48.816/2023 constará em documento anexo, separado e classificado conforme permissivo do mesmo normativo (art. 17, VIII).

32. JUSTIFICATIVA PARA ESCOLHA DO SISTEMA DE REGISTRO DE PREÇOS

32.1. De acordo com o art. 3º do Decreto 48.843/23, o SRP deverá ser adotado, preferencialmente, nas seguintes hipóteses:

I - quando a contratação se voltar ao atendimento de necessidade permanente, prolongada ou frequente do bem ou do serviço a ser contratado;

II - quando for mais conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida, por quantidade de horas de serviço ou postos de trabalho, ou em regime de tarefa;

III - quando for conveniente para atendimento a mais de um órgão ou entidade, bem como aos programas de governo; ou

IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

32.2. O Governo do Estado, como toda grande organização, tem gastos volumosos com produtos e serviços de Tecnologia da Informação e Comunicação (TIC) entre os órgãos que o compõe. Os crescentes desafios colocados para o governo acabam induzindo o aumento da máquina administrativa e, conseqüentemente, dos gastos com seus serviços. Desta forma, entendemos que o registro de preços se justifica, especialmente no que tange aos incisos I e III do referido Decreto.

32.3. Parte significativa desses dispêndios pode ser reduzida com processos de contratações eficientes, planejados previamente em conjunto por grupos de Órgãos. Além de melhorar a qualidade técnica dos artefatos de contratação, um planejamento integrado de contratação reduz a duplicidade de esforços entre os órgãos e otimiza o trabalho dos técnicos das áreas de licitações e contratos, ensejando ainda economia processual.

32.4. O grande benefício, entretanto, advém da utilização do poder de compra do governo. Na medida em que aproveita as oportunidades de economia de escala, a Administração Pública pode obter melhores preços junto ao mercado, reduzindo seus custos em benefício do atendimento às demandas sociais.

32.5. Esta é uma inteligência trazida pelo Sistema de Registro de Preços - SRP, utilizado sempre que conveniente à contratação de serviços para atendimento a vários Órgãos, que trabalham de forma integrada com suas estimativas de consumo e os aspectos técnicos da contratação.

32.6. Em suma, elencamos alguns argumentos que justificam a adoção do Sistema de Registro de Preços:

I - Melhoria da qualidade técnica dos documentos preliminares ao certame, tais como: especificações técnicas, alinhamento estratégico com o planejamento dos órgãos e condições jurídicas para a contratação;

II - Redução do esforço administrativo para a realização de diversos processos licitatórios sendo que a execução conjunta culmina em um único certame;

III - Redução de custos de manutenção e melhor eficiência pelo uso racional dos recursos, uma vez que estes foram definidos de forma a atender precisamente as necessidades do usuário;

IV - Ganho de economia de escala, pois, ao prospectar grandes volumes licitados, a Administração Pública amplia seu poder de compra junto aos fornecedores e consegue reduções consideráveis de preços, fato que certamente não ocorreria quando do fracionamento de certames.

32.7. Portanto, a utilização do Sistema de Registro de Preços será necessária neste certame, uma vez que atenderá as demandas do PRODERJ e demais órgãos da Administração Pública, podendo o quantitativo ora definido sofrer alterações, assim como está voltada para o atendimento de necessidade permanente, prolongada ou frequente do serviço.

33. INDICAÇÃO DO ÓRGÃO OU ENTIDADE GERENCIADOR DA ATA

33.1. Compete ao nível de Direção Geral, representado pelo PRODERJ, conduzir e disponibilizar, mas não limitado, atas de registro de preços, contratos e contratos corporativos para suprir itens relativos à TIC aos órgãos da administração pública de acordo com as políticas e diretrizes estabelecidas, tendo como objetivo a obtenção de ganhos e economia de escala para o Estado, além de benefícios intrínsecos de padronização e integração, conforme determina o inciso XIII, art. 3º do Decreto Estadual 48.997/2024.

33.2. Desta forma, o PRODERJ será o órgão Gerenciador.

34. INDICAÇÃO DOS ÓRGÃOS OU ENTIDADES PARTICIPANTES DA ATA

34.1. Após a realização de Intenção de Registro de Preços - IRP, os seguintes órgãos manifestaram pretensão de participar da licitação:

Órgãos Participantes da Ata de Registro de Preços - IRP 0494-2025 - WAAP						
ORGAOS	LOTE I					
	1 191788	2 191799	3 186917	4 186914	5 187045	6 186921
	Appliance de Web Application and API Protection (WAAP) - Hardware Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Appliance de Web Application and API Protection (WAAP) - Virtual Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Treinamento operacional para appliances WAAP	Subscrição de solução para proteção em nuvem (SaaS), incluindo instalação, configuração e suporte técnico por 12 meses.	Franquia adicional de tráfego limpo para o Item 4	Treinamento operacional para WAAP SaaS
PRODERJ	2	2	1	1	12	1
SEPLAG	1	2	2	0	0	0
SEPOL	2	0	1	0	0	0
SEPM	2	0	2	0	0	0
SEDEC	2	0	1	0	2	0
FAF	6	0	1	0	0	0
Quant. por Item	15	4	8	1	14	1
Quant. Total	43					

41.3. A quantidade estimada para os treinamentos considerou a capacitação, para os lotes I e II, de um grupo de até 8 (oito) técnicos de cada uma das três áreas técnicas (infraestrutura, sistemas e segurança da informação). Tais quantitativos consideraram o grau de relevância, na infraestrutura, das soluções tecnológicas às quais os treinamentos estão relacionados. Considerou ainda eventuais desligamentos de funcionários treinados, de forma a viabilizar o treinamento de novos funcionários.

41.4. A definição da franquia básica de dados inclusa no item de subscrição (item 4 do lote I), foi realizada com base nas contratações similares de WAAP SaaS, observadas no estudo técnico preliminar, onde as franquias básicas variavam entre 2 e 2.5 terabytes. Considerando que no momento, o PRODERJ praticamente não possui visibilidade sobre a volumetria de tráfego de dados em suas aplicações web, foi definida para esta contratação a maior franquia básica observada nas contratações similares, que era de 2.5 terabytes. Diante deste fator de imprevisibilidade, ao invés de adicionarmos um volume maior de dados para a franquia básica, nosso entendimento foi o de se criar um item distinto (item 5 do lote I), caso a volumetria pré-definida eventualmente não dê conta do tráfego gerado nas aplicações web.

41.5. A tabela dos Lotes I e II (WAAP e ADC) abaixo apresenta as quantidades estimadas da solução conforme as demandas do PRODERJ:

WAAP – LOTE I						
Item	ID SIGA	ID PCA-PNCP	Descrição	Métrica	Quantidade	Forma de quantificação
1	191788	24357	Appliance de Web Application and API Protection (WAAP) - Hardware Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	2	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
2	191799	24361	Appliance de Web Application and API Protection (WAAP) - Virtual Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	2	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
3	186917	23828	Treinamento operacional para appliances WAAP	Turma	1	Uma turma dá direito ao treinamento de 8 alunos.
4	186914	24354	Subscrição de solução para proteção em nuvem (SaaS), incluindo instalação, configuração e suporte técnico por 12 meses.	Anuidade	1	1 anuidade inclui: franquia mensal de 2.5 Terabytes de tráfego limpo, podendo ser consumido em até 25 aplicações (distribuídas em até 150 servidores).
5	187045	24355	Franquia adicional de tráfego limpo para o Item 4	TeraByte (TB)	12	A métrica do item é por terabyte, ou seja, basta informar a quantidade de terabytes adicionais que serão necessários.
6	186921	24356	Treinamento operacional para WAAP SaaS	Turma	1	Uma turma dá direito ao treinamento de 8 alunos.
ADC – LOTE II						
Item	ID SIGA	ID PCA-PNCP	Descrição	Métrica	Quantidade	Forma de quantificação
1	191789	24358	Appliance de Controle de Entrega de Aplicação (ADC) e Balanceamento Dinâmico de Carga, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	4	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.
2	188007	24359	Treinamento operacional para ADC	Turma	1	Uma turma dá direito ao treinamento de 8 alunos.

41.6. **Previsão de contratação pelo gerenciador e pelos participantes conforme IRP**

WAAP – LOTE I						
Item	ID SIGA	Descrição	Métrica	Quantidade	Forma de quantificação	
1	191788	Appliance de Web Application and API Protection (WAAP) - Hardware Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	15	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.	
2	191799	Appliance de Web Application and API Protection (WAAP) - Virtual Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	4	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.	
3	186917	Treinamento operacional para appliances WAAP	Turma	8	Uma turma dá direito ao treinamento de 8 alunos.	
4	186914	Subscrição de solução para proteção em nuvem (SaaS), incluindo instalação, configuração e suporte técnico por 12 meses.	Anuidade	1	1 anuidade inclui: franquia mensal de 2.5 Terabytes de tráfego limpo, podendo ser consumido em até 25 aplicações (distribuídas em até 150 servidores).	
5	187045	Franquia adicional de tráfego limpo para o Item 4	TeraByte (TB)	14	A métrica do item é por terabyte, ou seja, basta informar a quantidade de terabytes adicionais que serão necessários.	
6	186921	Treinamento operacional para WAAP SaaS	Turma	1	Uma turma dá direito ao treinamento de 8 alunos.	
ADC – LOTE II						
Item	ID SIGA	Descrição	Métrica	Quantidade	Forma de quantificação	
1	191789	Appliance de Controle de Entrega de Aplicação (ADC) e Balanceamento Dinâmico de Carga, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade	17	Sugerimos a aquisição de ao menos duas unidades, por conta de possíveis cenários de clusterização e/ou alta disponibilidade.	
2	188007	Treinamento operacional para ADC	Turma	6	Uma turma dá direito ao treinamento de 8 alunos.	

41.7. **Previsão de contratação pelos não-participantes**

PARÂMETRO	LOTE I						LOTE II	
	item 01 ID SIGA 191788	item 02 ID SIGA 191799	item 03 ID SIGA 186917	item 04 ID SIGA 186914	item 05 ID SIGA 187045	item 06 ID SIGA 186921	item 01 ID SIGA 191789	item 02 ID SIGA 188007
Quantidade máxima de contratação por meio de adesão (dobro da estimativa por item)	30	8	16	2	28	2	34	12

Quantidade máxima de contratação por órgão aderente (metade da estimativa por item)	7	2	4	1	7	1	8	3
---	---	---	---	---	---	---	---	---

41.8. As contratações adicionais pelos não-participantes não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens registrados na Ata de Registro de Preços para o gerenciador e para os participantes, quando houver.

41.9. O quantitativo decorrente das adesões à Ata de Registro de Preços não poderá exceder, na totalidade, ao limite de 200% (duzentos por cento) do quantitativo de cada item registrado na Ata para o gerenciador e para os participantes, quando houver, independentemente do número de órgãos ou entidades não-participantes que aderirem.

41.10. É vedada a participação do órgão ou da entidade em mais de uma Ata de Registro de Preços com o mesmo objeto no prazo de validade daquela de que já tiver participado, salvo na ocorrência de ata que tenha registrado quantitativo inferior ao máximo previsto no edital da licitação.

42. MATRIZ DE ALOCAÇÃO DE RISCOS

42.1. Observadas as condições constantes deste Termo de Referência, bem como o Mapa de Riscos realizado durante os Estudos Técnicos Preliminares, não se vislumbram riscos inerentes ao futuro contrato, os quais possam impactar no seu equilíbrio econômico-financeiro. Ademais, por se tratar de registro de preços, s.m.j., os riscos já estarão contingenciados na Ata de Registro de Preços, prescindindo a apresentação da matriz de riscos.

43. NECESSIDADE DE REALIZAÇÃO DE AUDIÊNCIA PÚBLICA

43.1. Será informada após a realização da pesquisa de preços, quando identificado o valor estimado para a contratação.

44. DISPOSIÇÕES FINAIS

44.1. O presente termo de referência foi concebido com base nas normas legais aplicadas à matéria e nas premissas recomendadas pelo Tribunal de Contas do Estado do Rio de Janeiro – TCE/RJ e a Procuradoria-Geral do Estado - PGE/RJ. Este documento constituirá parte integrante do edital da licitação a ser instaurado para viabilizar a contratação de empresa devidamente qualificada e que apresente o melhor preço para fornecimento dos serviços objeto desta demanda.

44.2. As empresas interessadas em participar da licitação serão integralmente responsáveis pela avaliação e levantamento dos custos relativos à execução do objeto, sendo inteiramente responsáveis por eventuais prejuízos decorrentes de avaliação equivocada ou da sua ausência.

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

45. ANEXOS

45.1. Abaixo, estão listados os documentos anexos cujas disposições estão em plena concordância com este Termo de Referência, do qual correspondem a parte integrante e indissociável:

- I - Especificações Técnicas do Objeto (112343713);
- II - Modelo de Relatório de Cumprimento do Objeto (112343334);
- III - Modelo de Termo de Confidencialidade e Sigilo (112344402);
- IV - Modelo de Ordem de Serviço / Autorização de Fornecimento (112344269);
- V - Modelo de Planilha de Composição de Preços (112344339);
- VI - Modelo de Termo de Recebimento Provisório (112344547);
- VII - Modelo de Termo de Recebimento Definitivo (112345156);
- VIII - Modelo de Declaração de Sustentabilidade Ambiental (112344648).

46. EQUIPE RESPONSÁVEL

Fabio Ivo Diretor de Segurança da Informação ID nº 5143032-0	Rosana Alves de Andrade Gerente de Proteção de Dados e Sistemas ID nº 4347470-5	Marco Antônio de Andrade Assessor-Chefe da Vice-Presidência de Administração ID nº 4284601-3	Charles Monteiro Guim Diretor de Patrimônio e Lo ID nº 4432892-3
---	--	--	---

Rio de Janeiro, 8 de setembro de 2025.



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:07, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112341703** e o código CRC **8EF4A86A**.



Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. INFORMAÇÕES PRELIMINARES

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

2. ESPECIFICAÇÕES TÉCNICAS DAS SOLUÇÕES DO LOTE 1

2.1. Contratação de empresa do ramo de Tecnologia da Informação para o fornecimento de solução Web Application and API Protection – WAAP em modalidade aquisição perpétua de hardware e software, com garantia de 36 (trinta e seis) meses, e subscrição de software por 12 (doze) meses, com instalação/configuração, suporte técnico e treinamento das soluções.

2.2. CARACTERÍSTICAS GERAIS DOS ITENS 1 e 2 DO LOTE 1 (WAAP)

2.2.1. Arquitetura

2.2.1.1. Deve ser fornecido em formato appliance, físicos ou virtuais, de acordo com o tipo especificado em cada item;

2.2.1.2. Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais;

2.2.1.3. Nenhum dos equipamentos fornecidos pode estar em modo End of Life, End of Sale e End of Support no dia do Pregão Eletrônico;

2.2.1.4. Suportar implementação em alta disponibilidade,

2.2.1.5. Implementar modo ativo/standby;

2.2.1.6. Suportar modo ativo/ativo para, pelo menos, as funções de proxy reverso. Aceita-se como ativo/ativo a utilização de dois endereços virtuais, onde cada endereço fica ativo em um elemento e standby no outro;

2.2.1.7. Permitir a sincronização das configurações de forma automática e manual, forçando a sincronização quando necessário;

2.2.1.8. Permitir utilizar qualquer endereçamento IP, inclusive os definidos na RFC 1918, para criação de cluster, heartbeat e sincronização entre os equipamentos;

2.2.1.9. Fornecer todos os recursos de redundância da solução sem nenhuma despesa com licenças adicionais;

2.2.1.10. Permitir expansão do cluster adicionando novos equipamentos inclusive de modelos diferentes;

2.2.1.11. Deve possuir suporte a Link Layer Discovery Protocol (LLDP), com, pelo menos, as informações: Port ID, TTL, Port Description, System Name, System Description, Management Address,

Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size;

2.2.1.12. Suportar exportação de informações de fluxos através sFlow, NetFlow, IPFIX ou outro protocolo similar;

2.2.1.13. Permitir a criação de códigos ou scripts capazes de manipular o tráfego, incluindo descartar, redirecionar, alterar, substituir e comparar valores e atributos, a partir de informações extraídas da conexão, sessão e protocolos;

2.2.1.14. Permitir utilizar listas de dados como fonte de dados por um script para validar se as conexões a serem estabelecidas obedecem a um dos critérios contidos nessa base de dados;

2.2.1.15. Suportar IPv4 e IPv6;

2.2.1.16. Suportar VXLAN para integração com o ambiente de virtualização;

2.2.1.17. Implementar roteamento IPv4 e IPv6 estático e dinâmico;

2.2.1.18. Suportar múltiplas tabelas de roteamento independentes em IPv4 e IPv6;

2.2.1.19. Suportar a criação de múltiplos domínios de roteamento, com tabelas de rotas isoladas, em IPv4 e IPv6, BGP, OSPF e RIP em IPv4 e IPv6;

2.2.1.20. Permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6;

2.2.1.21. Suportar integração via BGP para divulgação de prefixos;

2.2.1.22. Deve garantir que o retorno do tráfego seja encaminhado para o mesmo host que enviou o tráfego inicialmente para a solução, independente da configuração de rotas do equipamento. Por exemplo, no caso de múltiplos roteadores com acesso à Internet, a solução deve enviar o tráfego de retorno para o cliente sempre para o mesmo roteador que encaminhou o tráfego do cliente inicialmente para a solução;

2.2.1.23. Suportar Equal Cost Multipath (ECMP);

2.2.1.24. Implementar Bidirectional Forward Detection (BFD);

2.2.1.25. Deve possuir Proteção contra DDoS, Firewall de Aplicação, Gerenciamento e Proteção de DNS, Mitigação de Bots.

2.2.2. **Gerenciamento**

2.2.2.1. Possuir interface gráfica via web e interface via CLI por SSH e console para administração, gerenciamento e monitoramento do equipamento;

2.2.2.2. Suportar configuração de endereçamento IP estático e dinâmico (DHCP/BOOTP) para o gerenciamento;

2.2.2.3. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol);

2.2.2.4. Permitir habilitar e desabilitar acesso administrativo via SSH por qualquer interface do equipamento;

2.2.2.5. Manter internamente múltiplos arquivos de configurações do sistema;

2.2.2.6. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e sistema operacional;

2.2.2.7. Possuir recurso de autocompletar nos comandos na CLI, com ajuda contextual;

2.2.2.8. Permitir a configuração de múltiplas contas locais de administradores;

2.2.2.9. Implementar controles de acesso por nível, os quais podem ser atribuídos a usuários ou grupos de usuários para fazer cumprir a separação por perfil de privilégios;

2.2.2.10. Possuir, no mínimo, três níveis de usuários na GUI: administrador, analista e somenteleitura;

2.2.2.11. Suportar autenticação e autorização externa de usuários administradores através de RADIUS, LDAP, Active Directory e TACACS+;

- 2.2.2.12. A interface gráfica deve permitir a atualização do sistema operacional, atualização de componentes e instalação de patches;
- 2.2.2.13. Permitir selecionar pela interface gráfica a versão do sistema operacional para inicialização do equipamento;
- 2.2.2.14. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps);
- 2.2.2.15. Suportar a rollback de configuração e imagem;
- 2.2.2.16. Possuir o registro local de eventos relevantes do sistema e suportar o envio via syslog de eventos relevantes ao sistema, com capacidade de configuração de múltiplos servidores de syslog;
- 2.2.2.17. Implementar rate limit da taxa logs enviados para servidores externos, com o objetivo de prevenir a sobrecarga e perda de logs por motivos de alta utilização de CPU, memória ou uso de banda;
- 2.2.2.18. Permitir reiniciar o equipamento pela interface gráfica e por CLI;
- 2.2.2.19. Implementar SNMPv1, SNMPv2c e SNMPV3;
- 2.2.2.20. Implementar traps SNMP;
- 2.2.2.21. Possuir agente integrado de coleta e exportação de métricas de desempenho e eventos:
- I - Coleta de métricas de desempenho compatível com Prometheus;
 - II - Coleta de métricas de desempenho em formato JSON utilizando cliente HTTP;
 - III - Exportação de métricas de desempenho compatíveis com, pelo menos, os sistemas AWS CloudWatch e S3, Azure Log Analytics e Application Insights, ElasticSearch, Fluentd, GCP Cloud Monitoring e Logging, Graphite, Kafka, Splunk e StatsD;
 - IV - Exportação de eventos da solução compatível com, pelo menos, os sistemas AWS S3, Azure Log Analytics, ElasticSearch, Fluentd, GCP Cloud Logging, Graphite, Kafka e Splunk;
 - V - Exportação de métricas de desempenho em formato JSON para um servidor HTTP;
 - VI - Permitir definir critérios de inclusão e exclusão de coleta e exportação de métricas;
 - VII - Deve incluir métricas de desempenho relacionadas a servidores virtuais, pool e pool members;
 - VIII - Deve incluir métricas de throughput, conexões, bits, pacotes, disponibilidade;
 - IX - Deve incluir métricas de requisições, respostas;
 - X - Deve incluir métricas de criptografia, incluindo cifras, algoritmos, versão, conexões, bytes criptografados, bytes descriptografados;
 - XI - Deve incluir métricas de certificados digitais, incluindo data de expiração, issuer e subject;
 - XII - Deve incluir métricas relacionadas a CPU, memória, discos e interfaces;
 - XIII - Deve incluir métricas de desempenho dos scripts de manipulação de tráfego, incluindo total de execuções, média de ciclos, máximo e mínimo de ciclos e falhas;
 - XIV - Deve incluir informações de inventário (hostname, id, versão, localização, plataforma, chassi, módulos provisionados);
 - XV - Deve incluir métricas do cluster, incluindo data de sincronização;
 - XVI - Deve incluir informações de data da última configuração aplicada.
- 2.2.2.22. Deve possuir documentação pública do fabricante contendo informações de configurações, exemplos de configuração e modelos de mensagens;
- 2.2.2.23. Implementar debugging utilizando CLI via console e SSH;

- 2.2.2.24. Possuir ferramenta interna nativa de captura de tráfego de rede com informações contextuais da solução inseridas em cada pacote/frame;
- 2.2.2.25. Permitir a exportação de informações de diagnóstico, logs, configurações, desempenho para análises externas sem interferência na solução em produção. A análise deve ser feita em ferramenta, disponível sem custo adicional, online via web ou via aplicação para Windows, Linux ou MacOS;
- 2.2.2.26. Possuir API REST para configuração de servidores virtuais, políticas de segurança, parâmetros, perfis e demais configurações;
- 2.2.2.27. Possuir integração com esteiras de automação que permita que as configurações sejam realizadas de forma automática e dinâmica, de forma declarativa, por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;
- 2.2.2.28. Possuir relatórios do serviço de DNS incluindo tendência de latência de resposta de DNS, nomes de domínios de DNS mais requisitados, tendência de uso do cache de DNS, clientes de DNS, clientes por domínio de DNS, taxa de consultas de DNS por tipo de registro, taxa de consultas de DNS diária por servidor, pico de consultas diárias de DNS por servidor, NXDOMAIN, SERVFAIL enviados e recebidos, nomes de domínios com conteúdo malicioso, principais domínios maliciosos;
- 2.2.2.29. Possuir relatórios de proteção do serviço de DNS, incluindo eventos por período, eventos por severidade, eventos por regra, eventos por tendência e eventos por categoria;
- 2.2.2.30. Suportar a exportação de eventos de DNS utilizando IPFIX;
- 2.2.2.31. Deve possuir relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DDoS;
- 2.2.2.32. Possuir relatório de ataques DDoS com indicação de início e fim do ataque;
- 2.2.2.33. Possuir relatório em tempo real sobre ataques DDoS, atualizado automaticamente;
- 2.2.2.34. Possuir relatório de ataques DDoS incluindo quantidade de eventos e severidade, ataques por protocolo, incluindo assinaturas utilizadas e serviços mais afetados;
- 2.2.2.35. Possuir relatórios de ataques DDoS incluindo a origem dos ataques, país, requisições por segundo, gatilho da proteção e mitigação adotada;
- 2.2.2.36. Suportar a exportação de eventos de DDoS utilizando IPFIX;
- 2.2.2.37. Possuir painel de acompanhamento de adoção de proteções contra ameaças mais comuns, de acordo com OWASP Top 10 2021;
- 2.2.2.38. Possuir relatório de desempenho da solução, incluindo processamento total e por servidor virtual protegido;
- 2.2.2.39. Possuir relatórios consolidados de ataques incluindo, pelo menos, resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, ataques DDoS, ataques de força bruta, ataques de bots, violações, URL, endereços IP, países e severidade;
- 2.2.2.40. Possuir relatório de incidentes com violações detectadas e correlacionadas, separando falsos positivos de atividades maliciosas e para facilitar a resposta a incidentes;
- 2.2.2.41. Implementar monitoração e análise de performance de aplicações web;
- 2.2.2.42. Possuir relatórios de métricas de aplicações, incluindo transações por segundo, tempo de resposta, latência do cliente e servidor, throughput de requisição e resposta e sessões;
- 2.2.2.43. Possuir relatórios de análises históricas detalhamento do tempo de resposta total de carregamento de uma URL e página e correlação de métricas de uso de rede com o comportamento das aplicações para auxiliar processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;
- 2.2.2.44. Possuir relatórios para análise de dados por aplicações, por URL, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução;
- 2.2.2.45. Possuir relatórios para análise de estatísticas de acesso, incluindo métodos HTTP, sistema

operacional e navegadores;

- 2.2.2.46. Permitir exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário
- 2.2.2.47. Possuir relatório de ataques DDoS em camada 7 com indicação de início e fim do ataque;
- 2.2.2.48. Possuir relatório em tempo real sobre ataques DDoS em camada 7, atualizado automaticamente;
- 2.2.2.49. Possuir relatório que permite avaliar o impacto de ataques DDoS em camada 7 na performance do servidor;
- 2.2.2.50. Implementar funções de entrega de aplicações através do balanceamento de servidores com qualquer hardware, sistema operacional e tipo de aplicação;
- 2.2.2.51. Suportar os protocolos HTTP/1.0, HTTP/1.1, HTTP/2 e HTTP/3, para comunicação com o cliente e comunicação com o servidor;
- 2.2.2.52. Implementar a reutilização de conexões entre a solução e os servidores, para diferentes clientes e diferentes requisições;
- 2.2.2.53. Suportar os métodos de balanceamento round robin, least connections, weighted (por peso), tempo de resposta mais rápida baseado no tráfego real, baseado em parâmetros dinâmicos coletados via SNMP ou WMI;
- 2.2.2.54. Implementar criptografia de cookies;
- 2.2.2.55. Implementar persistência com pelo menos os métodos por cookie inserindo um novo cookie na sessão, por cookie utilizando um valor do cookie da aplicação, sem adição de cookie, por endereço IP destino, por endereço IP origem, por sessão SSL, parâmetros da URL acessada, parâmetro no header HTTP, qualquer informação do payload camada 7;
- 2.2.2.56. Permitir configuração de grupos de servidores secundários que devem ser utilizados para balanceamento somente quando uma quantidade mínima especificada de servidores estiver disponível no grupo primário. Caso o número de servidores disponíveis fique menor do que o especificado, a solução deve automaticamente distribuir o tráfego para o próximo grupo. Caso o número de servidores disponíveis volte ao valor mínimo, a solução deve automaticamente voltar a utilizar o grupo primário de servidores;
- 2.2.2.57. Permitir a replicação do tráfego destinado a servidores virtuais, permitindo habilitar a cópia do tráfego entre o cliente e a solução e entre a solução e o servidor;
- 2.2.2.58. Implementar pelo menos monitores de servidores de servidores via ICMP, conexões TCP e UDP pela respectiva porta no servidor e HTTP e HTTPS, incluindo HTTP/2;
- 2.2.2.59. Suportar balanceamento de carga de servidores SIP para VoIP;
- 2.2.2.60. Permitir limitar o número de conexões estabelecidas com cada servidor real;
- 2.2.2.61. Permitir limitar o número de conexões estabelecidas com cada servidor virtual;
- 2.2.2.62. Implementar Network Address Translation (NAT) do IP do servidor;
- 2.2.2.63. Implementar Network Address Translation (NAT) do IP do cliente;
- 2.2.2.64. Implementar proteção contra Denial of Service (DoS) em camada 3, 4 e 7;
- 2.2.2.65. Implementar proteção contra SYN floods;
- 2.2.2.66. Suportar servidores virtuais com endereço IPv4 e os servidores reais com endereços IPv6;
- 2.2.2.67. Suportar multiplexação TCP e reuso de sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados;
- 2.2.2.68. Suportar Stream Control Transmission Protocol (SCTP);
- 2.2.2.69. Implementar aceleração de TLS com instalação do certificado digital na solução, troca de chaves e criptografia dos dados;
- 2.2.2.70. Permitir recriptografar a conexão entre a solução e o servidor;

- 2.2.2.71. Permitir espelhamento de tráfego de conexões TLS;
- 2.2.2.72. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2 (SHA256/384) e ChaCha20-Poly1305;
- 2.2.2.73. Em relação ao tráfego TLS, deve suportar:
- I - Autenticação do servidor pelo cliente, apresentando um certificado previamente configurado;
 - II - Autenticação do cliente pela solução, através da solicitação e verificação do certificado fornecido pelo cliente;
 - III - Autenticação mútua (mTLS), quando ambas as autenticações acima mencionadas ocorrem. Durante a autenticação com mTLS, a solução deve apresentar para o servidor um certificado de cliente com atributos extraídos do certificado original obtido do cliente, preservando a autenticação mútua fim a fim;
 - IV - Encaminhar ao servidor real via cabeçalho HTTP todo o certificado utilizado pelo cliente para se autenticar;
 - V - Encaminhar ao servidor real via cabeçalho HTTP atributos específicos do certificado utilizado pelo cliente.
- 2.2.2.74. Suportar os algoritmos para sessões TLS:
- I - SSL session cache Timeout;
 - II - Session Ticket;
 - III - OCSP (Online Certificate Status Protocol) Stapling;
 - IV - Dynamic Record Sizing;
 - V - ALPN (Application Layer Protocol Negotiation); VI - Perfect Forward Secrecy.
- 2.2.2.75. Suportar múltiplos certificados digitais no mesmo servidor virtual, com identificação via SNI (Server Name Indication);
- 2.2.2.76. Suportar importação de certificados digitais e chaves privadas;
- 2.2.2.77. Possuir alertas visuais na interface web de certificados com vencimento próximo;
- 2.2.2.78. Implementar limpeza de cabeçalho HTTP;
- 2.2.2.79. Implementar compressão de conteúdo HTTP, suportar os algoritmos gzip e deflate e permitir definir compressão especificamente para certos tipos de objetos;
- 2.2.2.80. Permitir a criação de políticas para classificação de tráfego através de parâmetros da aplicação, incluindo informações de geolocalização IP, cabeçalhos de autenticação HTTP, cookies e operações de cookie, cabeçalhos HTTP, host, método, Referer, Status Code e URI;
- 2.2.2.81. Permitir as ações para o tráfego classificado: bloqueio, reescrita e manipulação de URL, adicionar cabeçalho HTTP, redirecionar o tráfego para um servidor específico, escolher uma política de proteção web, logging do tráfego;
- 2.2.2.82. Suportar log de todas as sessões e permitir a customização do formato, incluindo endereço IP de origem, Porta TCP e UDP de origem, endereço IP de destino, porta TCP e UDP de destino, protocolo de camada 4 (TCP ou UDP), data e hora da mensagem, URL acessada;
- 2.2.2.83. Implementar o envio de dados de análises e desempenho relacionados ao TCP e HTTP;
- 2.2.2.84. Permitir utilizar diferentes configurações de envio de eventos de uma mesma aplicação, de forma que eventos válidos sejam enviados para um servidor e eventos de violações de segurança sejam enviados para outro servidor;
- 2.2.2.85. Permitir exportar eventos de acesso para servidores externos com configuração das informações exportadas;

2.2.2.86. Permitir a configuração de autenticação e autorização de clientes HTTP, através de base LDAP, RADIUS e certificados digitais;

2.2.2.87. Implementar integração com ambientes de orquestração de containers para criação dinâmica de serviços de entrega de aplicações e balanceamento de carga na solução, modificando a configuração de forma dinâmica e automática a partir de configurações feitas na plataforma de orquestração; considerando:

I - Suportar, pelo menos, as plataformas Kubernetes “Vanilla”, Red Hat OpenShift e VMware Tanzu;

II - Permitir a configuração através de ConfigMaps;

III - Permitir a configuração através de CustomResourceDefinition (CRD) da solução;

IV - Permitir a configuração através de objetos Ingress na plataforma;

V - Permitir a configuração através de objetos Route no OpenShift;

VI - Permitir incluir serviços de entrega de aplicações da solução, tais como SSL Offload e proteção de aplicações;

VII - A solução deverá receber e realizar automaticamente as alterações do ambiente e atualizações de pool de pods ou nodes disponíveis para o serviço publicado de acordo com a integração realizada.

2.2.2.88. Suportar o protocolo FTP com, pelo menos, as seguintes características:

I - Determinar os comandos FTP permitidos;

II - Requests FTP anônimos;

III - Validar conformidade com o protocolo FTP;

IV - Proteger de ataques de força bruta nos logins;

V - Suportar o protocolo SMTP com, pelo menos, as seguintes características:

a) Limitar o número de mensagens;

b) Validar registro SPF do DNS;

c) Determinar quais métodos SMTP podem ser utilizados.

2.2.2.89. Implementar proteção de aplicações no nível de rede e protocolo;

2.2.2.90. Permitir implementação no modo que todo o tráfego seja bloqueado com exceções explícitas em regras de permissões e no modo que todo tráfego é permitido com exceções explícitas em regras de bloqueio.

2.2.3. **Mitigação de Ataques Distribuídos de Negação de Serviço (DDoS)**

2.2.3.1. Proteger de ataques DDoS nas camadas de rede e de sessão;

2.2.3.2. Proteger de ataques DDoS que utilizem SSL;

2.2.3.3. A solução deve permitir a criação de regras com, no mínimo, os parâmetros:

I - Endereço IP de destino;

II - Endereço IP de origem;

III - Porta de destino;

IV - Porta de origem;

V - VLAN;

VI - Protocolo;

VII - Ação;

VIII - Horário;

IX - Log;

- 2.2.3.4. Permitir definir agendamento para ativação da regra;
- 2.2.3.5. Permitir criar regras com base em zonas de segurança e por interface ou VLAN;
- 2.2.3.6. Implementar a descoberta automática de serviços presentes em objetos monitorados;
- 2.2.3.7. Permitir definir, no mínimo, as seguintes ações no tráfego:
- I - Permitir: os pacotes são aceitos e passam pela solução;
 - II - Rejeitar: os pacotes são rejeitados e ocorre envio de pacotes de destino inatingível ou similar a origem do tráfego;
 - III - Descartar: onde os pacotes são descartados sem o envio de qualquer notificação a origem do tráfego.
- 2.2.3.8. Deve ser possível criar regras que sejam aplicadas em diferentes hierarquias, incluindo, no mínimo:
- I - Global, regras válidas para todo o tráfego, independente da interface de ingresso;
 - II - Domínio de roteamento, regras válidas para todo o tráfego daquele domínio, independente da interface de ingresso;
 - III - Objeto, regras válidas para objetos específicos.
- 2.2.3.9. Deve possuir criptografia IPSEC para comunicação entre sites;
- 2.2.3.10. Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de limiares baseados no perfil de rede ou através de limites de tráfego atingido;
- 2.2.3.11. Permitir a restauração das configurações de proteções originais;
- 2.2.3.12. Deve permitir criar lista de exceção de regras por endereço IP específico ou faixa de subrede;
- 2.2.3.13. Permitir a criação de códigos ou scripts para customizar e aumentar o nível de segurança contra DDoS;
- 2.2.3.14. Permitir o consumo de listas externas de IPs para bloqueio com base em destino e origem, com atualização automática e ajuste manual da frequência de atualização;
- 2.2.3.15. Permitir o acionamento via API do descarte de conexões (shun) para integração com terceiros, tais como SIEM, IPS, IDS e outros;
- 2.2.3.16. Permitir a criação de regras de filtragem através de API REST declarativa; considerando:
- I - A documentação da API deve ser pública.
- 2.2.3.17. Exibir uma lista de proteções ativas juntamente com estatísticas resumidas sobre as quantidades de tráfego descartado e aceito;
- 2.2.3.18. Incluir informações estatísticas sobre o tráfego total e o total bloqueado por cada tipo de prevenção;
- 2.2.3.19. Implementar proteção contra pacotes inválidos, incluindo verificação para DNS malformed, Bad ICMP Frame, Bad ICMP Checksum, ICMP Frame too Large, Bad IGMP Frame, Bad IP TTL Value, Bad IP Version, Header Length Too Short, Bad Source, Bad IPV6 Hop Count, Bad IPV6 Version, Bad TCP Checksum, Bad TCP Flags, SYN & FIN Set, Bad UDP Checksum, ARP Flood, ICMPv4 Flood, ICMPv6 Flood, IGMP Flood, IGMP Fragment Flood, TCP RST Flood, TCP SYN ACK Flood, TCP SYN Flood, UDP Flood, SIP ACK Method, SIP Malformed, Single Endpoint Flood, Single Endpoint Sweep, LAND Attack, DNS Water-torture e fornecer estatísticas para os pacotes descartados;
- 2.2.3.20. Implementar descarte de sessões TCP ociosas se o cliente não enviar uma quantidade de dados dentro de um período configurável;

- 2.2.3.21. Limitar o número de consultas DNS por segundo através da configuração de limiares;
- 2.2.3.22. Mitigar, no mínimo, os tipos de ataques ICMP/UDP/TCP Flood, TCP Flag Abuse, GET/POST Flood, SYN Flood, UDP Bandwidth Attack, Smurfing, NTP Reflection Attack, TCP/UDP Bandwidth Attack, Fragging Attack, Slowloris, Connection Attack e Fragmentation Attacks;
- 2.2.3.23. Possuir recurso de bloqueio automático e temporário de atacantes, devendo ser possível especificar o tempo mínimo para iniciar o bloqueio e o tempo de bloqueio;
- 2.2.3.24. Suportar envio de SNMP traps para cada ataque DDoS detectado;
- 2.2.3.25. Possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes;
- 2.2.3.26. Deve possuir a funcionalidade de limiares automático para vetores de DDoS:
 - I - Essa funcionalidade deve valer tanto para proteção geral como também para proteção de serviços específicos.
 - II - Os limiares automáticos serão construídos pelo próprio sistema e aplicados aos diversos vetores de ataques selecionados.
- 2.2.3.27. Permitir configurar o sistema para detectar e mitigar assinaturas dinâmicas, capaz de detectar possíveis ameaças de DDoS baseado no histórico e comportamento do tráfego e mitigar automaticamente essas ameaças;
- 2.2.3.28. Suportar integração com serviço de tratamento de DDoS externo através do compartilhamento de informação de vetores e sinalização de ataques em andamento para redirecionamento de tráfego via BGP (BGP FlowSpec) e limpeza do tráfego em centros de limpezas externos.

2.2.4. **Gerenciamento e Proteção de DNS**

- 2.2.4.1. Implementar serviços de entrega de aplicações distribuídas através do serviço de DNS;
- 2.2.4.2. Implementar serviços de DNS com as funções de DNS autoritativo, DNS secundário, DNS resolver, DNS cache e balanceamento de servidores de DNS;
- 2.2.4.3. Implementar DNSSec, independente da estrutura dos servidores DNS em uso;
- 2.2.4.4. Implementar transferência de zonas para múltiplos servidores DNS primários responsáveis por diferentes zonas;
- 2.2.4.5. Suportar uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;
- 2.2.4.6. Implementar offload dos servidores de DNS, funcionando como o DNS secundário;
- 2.2.4.7. Implementar proteções contra-ataques DNS, incluindo no mínimo a inspeção de protocolo, validação de protocolo, UDP flood, pacotes malformados, teardrop e DNS Water-torture;
- 2.2.4.8. Permitir a criação de códigos ou scripts que possam manipular as respostas de DNS;
- 2.2.4.9. Implementar filtragem de pacotes e tipos de requisições;
- 2.2.4.10. Implementar segurança do protocolo DNS, protegendo de ataques de negação de serviço, NXDOMAIN, reflexão e amplificação de DNS e Cache Poisoning;
- 2.2.4.11. Implementar stateful inspection das requisições e respostas de DNS;
- 2.2.4.12. Possuir base de geolocalização IP;
- 2.2.4.13. Implementar DNS64:
 - I - Implementar a tradução de IPv4 (A) para IPv6 (AAAA) utilizando um prefixo pré-definido;
 - II - Implementar a consulta em servidor recursivo IPv4 (A) e responde a tradução de
 - III - IPv4 (A) para IPv6 (AAAA) utilizando um prefixo pré-definido;

IV - Implementar a resposta da consulta diretamente em IPv6 (AAAA);

V - Implementar o encaminhamento da resposta de um recursivo diretamente em IPv6 (AAAA);

VI - Permitir configurar diferentes prefixos para respostas IPV6 (AAAA).

2.2.4.14. Implementar filtros para tipos de requisição, de forma que apenas as operações e requisições autorizadas sejam encaminhadas para os servidores de DNS.

2.2.4.15. Suportar pelo menos os tipos de requisição SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV e TXT;

2.2.4.16. Suportar DNS over HTTPS (DoH);

2.2.4.17. Permitir a criação de resoluções de DNS com tratamento diferenciado de consultas conforme origem das requisições;

2.2.4.18. Apresentar estatísticas sobre consultas de DNS por aplicação, nome da query, tipo da query, endereço IP do cliente;

2.2.4.19. Implementar modo inline na estrutura de DNS existente e transparente;

2.2.4.20. Suportar IP Anycast;

2.2.4.21. Implementar alta disponibilidade de Data Centers sem depender de BGP ou outro protocolo de roteamento;

2.2.4.22. Implementar alta disponibilidade de Data Centers e serviços baseada em respostas a requisições DNS, de forma que a resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas;

2.2.4.23. Suportar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição;

2.2.4.24. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido;

2.2.4.25. Suportar monitores utilizando HTTPS, incluindo a validação do SNI;

2.2.4.26. Suportar pelo menos os algoritmos de balanceamento round robin, disponibilidade, peso, persistência do LDNS, geolocalização, round trip time e hops;

2.2.4.27. Implementar persistência da conexão do usuário entre aplicações ou data centers;

2.2.4.28. Suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo;

2.2.4.29. Permitir que as políticas sejam configuradas individualmente por aplicação que será balanceada;

2.2.4.30. Permitir que a contingência seja automática;

2.2.4.31. Permitir o retorno do Data Center de forma automática e manual;

2.2.4.32. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requisições AAAA);

2.2.4.33. Possuir suporte a IPv6 no balanceamento global entre datacenters;

2.2.4.34. Possuir a funcionalidade de resposta rápida a requisições de DNS, permitindo respostas mais rápidas para zonas que seja autoritativo;

2.2.4.35. Suportar Response Policy Zones (RPZ), mecanismo de proteção de resolução para DNS recursivo que permite o tratamento customizado da resolução de nomes, capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas;

2.2.4.36. Suportar EDNS-Client-Subnet (ECS) para tanto responder requisições de clientes para balanceamento de Data Center ou encaminhar requisições de clientes.

2.2.4.37. Implementar a utilização da subnet do cliente presente no ECS para tomada de decisão de

balanceamento de Data Center, independente do endereço do LDNS;

2.2.4.38. Suportar inserir o ECS para outros servidores DNS;

2.2.4.39. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver, deve ser usada a persistência existente para manter o cliente no mesmo Data Center;

2.2.4.40. Permitir consultar a resposta de uma resolução de DNS em uma base de IP e permitir que a resposta seja alterada antes de ser enviada para o cliente;

2.2.4.41. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso, incluindo IP de origem, destino, data e hora do acesso.

2.2.4.42. Suportar, no mínimo, as ações de apenas registrar, bloquear o dado ou substituir o nome do domínio;

2.2.4.43. Permitir configurar rate limit realizadas via TCP ou UDP por FQND;

2.2.4.44. Permitir configurar rate limit para consultas realizadas via TCP ou UDP por IP de origem.

2.2.5. **Proteção de BOTs**

2.2.5.1. Implementar detecção com base na validação do cliente através de código executado no navegador para identificação de bots;

2.2.5.2. Não serão aceitas soluções que utilizam apenas o user-agent para detecção de bots;

2.2.5.3. Implementar proteção proativa de ataques automatizados por bots e outras ferramentas, como web scrapers.

2.2.5.4. Possuir atualização automática de definição de bots;

2.2.5.5. Permitir a configuração de bloqueio e permissão de bots benignos conhecidos, como Google, Yahoo! e Microsoft Bing;

2.2.5.6. Permitir a criação de definições de bots;

2.2.5.7. Implementar detecção e mitigação para proteção contra bots através da combinação de desafios enviados ao navegador do usuário e técnicas avançadas de análise.

2.2.6. **Proteção de Aplicações e API's**

2.2.6.1. Deve implementar proteção para aplicações web e API contra ameaças na camada de aplicação;

2.2.6.2. Possuir tecnologia para mitigação de DDoS em camada 7 a partir de análises comportamentais;

2.2.6.3. Implementar ajustes automáticos e adaptativos de limiares de DDoS;

2.2.6.4. Permitir a captura automática do tráfego relativo a ataques DDoS em camada 7, web scraping e força bruta;

2.2.6.5. Implementar proteção para aplicações web contra ameaças listadas no OWASP Top 10 (2021) e OWASP API Security Top 10 (2023);

2.2.6.6. Implementar modelo positivo de segurança de aplicações web;

2.2.6.7. Implementar modelo negativa de segurança, ou seja, adotar assinatura de ataques, ameaças e exploração de vulnerabilidade, de aplicações web;

2.2.6.8. Possuir conjuntos de configurações de segurança pré-definidas para configuração rápida de políticas;

2.2.6.9. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;

- 2.2.6.10. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- 2.2.6.11. Permitir desativar a inspeção para URL específicas;
- 2.2.6.12. Implementar identificação do usuário da aplicação web, mantendo a identificação até que o usuário tenha deixado o aplicativo;
- 2.2.6.13. Permitir a integração com firewall de banco de dados;
- 2.2.6.14. Suportar aplicações que utilizam protocolo WebSocket;
- 2.2.6.15. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0, mantendo a versão do protocolo para comunicação com o cliente e comunicação com o servidor, e sem a necessidade de downgrade de versão;
- 2.2.6.16. Implementar, no mínimo, proteção contra:
- I - Acesso por força bruta;
 - II - DDoS em camada 7;
 - III - Buffer Overflow;
 - IV - Cross Site Request Forgery (CSRF);
 - V - Cross-Site Scripting (XSS);
 - VI - Server-Side Request Forgery (SSRF);
 - VII - SQL Injection;
 - VIII - Parameter tampering;
 - IX - Cookie poisoning;
 - X - HTTP Request Smuggling;
 - XI - Manipulação de campos escondidos (hidden input);
 - XII - Manipulação de cookies;
 - XIII - Roubo de sessão através de manipulação de cookies;
 - XIV - Sequestro de sessão;
 - XV - Validação de consistência de formulários;
 - XVI - Validação do cabeçalho do “user-agent” para identificar clientes inválidos.
- 2.2.6.17. Permitir especificar quais URLs devem ser utilizadas para proteção contra CSRF (CrossSite Request Forgery);
- 2.2.6.18. Suportar codificação HTML "application/x-www-form-urlencoded";
- 2.2.6.19. Suportar HTTP Batched Request com proteções e assinaturas considerando individualmente URIs, cabeçalhos e conteúdo;
- 2.2.6.20. Suportar codificação fragmentada (chunked encoding);
- 2.2.6.21. Suportar validações de protocolo:
- I - Restrição de métodos;
 - II - Restrição de protocolos e versões;
 - III - Validação de conformidade com RFCs;
 - IV - Validação de caracteres URL-encoded;
 - V - Validação de codificação fora de padrão %uXXYY.
- 2.2.6.22. Suportar validações de HTML com nome de parâmetros, tamanho e tipo dos valores de parâmetros e combinação de nome, tipo e tamanho de parâmetros;
- 2.2.6.23. Possuir técnicas de detecção de evasões:

- I - URL-decoding;
 - II - Terminação Null Byte String;
 - III - Paths autorreferenciados;
 - IV - Case de caracteres misturados;
 - V - Uso excessivo de espaços em branco;
 - VI - Decodificação de entidades HTML; VII - Caracteres de escape.
- 2.2.6.24. Permitir a inspeção externa de arquivos enviados por usuários (upload) para os servidores de aplicação utilizando Internet Content Adaptation Protocol (ICAP);
- 2.2.6.25. Capacidade de filtrar cabeçalhos, corpo e status de respostas;
- 2.2.6.26. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;
- 2.2.6.27. Implementar validação de URL; considerando:
- I - Validação de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT) por URL;
- 2.2.6.28. Implementar proteção de aplicações web que utilizam chamadas de API, protegendo tanto a aplicação como a API, com a visibilidade que se trata da mesma sessão de usuário;
- 2.2.6.29. Suportar aplicações Single-Page Application (SPA);
- 2.2.6.30. Permitir a customização da resposta de bloqueio;
- 2.2.6.31. Permitir a configuração de lista de exceções temporárias ou permanentes de endereços IP bloqueados;
- 2.2.6.32. Permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem limites estabelecido, por um período configurável;
- 2.2.6.33. Permitir implementar:
- I - Proteção contra exposição de informações do ambiente e servidores internos como, sistema operacional e servidor web;
 - II - Ocultação de mensagem de erro HTTP;
 - III - Remoção de mensagens de erro às páginas que serão enviadas aos usuários;
- 2.2.6.34. Suportar políticas por geolocalização para restrição de acesso a determinados países;
- 2.2.6.35. Implementar aprendizado automático para identificação da estrutura da aplicação, incluindo URLs, parâmetros URLs, campos de formulários, tipo de dado, tamanho de caracteres, cookies;
- 2.2.6.36. O aprendizado deve ser capaz de diferenciar atributos com o mesmo nome, mas presentes em URLs diferentes;
- 2.2.6.37. Implementar aprendizado automático de XML;
- 2.2.6.38. Permitir a importação de arquivo de esquema XML;
- 2.2.6.39. Implementar aprendizado automático de JSON;
- 2.2.6.40. Permitir a importação de arquivo de esquema JSON;
- 2.2.6.41. Permitir a criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real;
- 2.2.6.42. Permitir ajustar parâmetros de tempo e origem de aprendizado;
- 2.2.6.43. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- 2.2.6.44. Implementar detecção e mitigação de ameaças e ataques com base em assinaturas de ataques, com atualização periódica e automática da base de assinaturas;
- 2.2.6.45. As assinaturas devem ser atualizadas durante o período do contrato, sem custo adicional; considerando:

I - Não serão aceitas soluções que definem assinaturas como sendo uma base de reputação de IP;

II - A atualização deve ser relacionada apenas as assinaturas, não sendo aceitas soluções que demanda a atualização do sistema operacional para atualização de cada nova versão da base de assinaturas.

2.2.6.46. Permitir a configuração automática de assinaturas com base em uma lista interna de tecnologias utilizadas pela aplicação;

2.2.6.47. Permitir desabilitar assinaturas específicas para determinados parâmetros, se comportando como exceção da configuração geral da política;

2.2.6.48. Permitir configurar um período de adaptação de novas assinaturas, quando nenhuma requisição que viole a assinatura deve ser bloqueada, apenas informada em relatório. Este processo deve ser automático, não sendo necessário a criação de regras específicas a cada atualização de assinatura;

2.2.6.49. Possuir assinaturas de ataques para conteúdo em JSON e XML;

2.2.6.50. Possuir proteções contra XML Bomb;

2.2.6.51. Possuir proteção para WebServices, suportar WS-I Basic Profile, importação de WSDL e aplicação de controles, criptografar e descriptografar partes das mensagens SOAP, assinar digitalmente e verificar de partes das mensagens SOAP;

2.2.6.52. Possuir integração com soluções externas de análise vulnerabilidade para importação de relatórios e configuração de políticas de segurança, indicando quais vulnerabilidades podem ser resolvidas e quais devem ser resolvidas manualmente externamente;

2.2.6.53. Implementar detecção de DDoS na camada 7, através de análise comportamental, com aprendizado automático do comportamento da aplicação e combinação com nível de carga do servidor;

2.2.6.54. Permitir apenas registrar o ataque, sem tomar nenhuma ação de bloqueio;

2.2.6.55. Implementar detecção com base no número de requisições por segundo enviados a uma URL específica;

2.2.6.56. Implementar detecção com base no número de requisições por segundo enviados de um IP específico;

2.2.6.57. Implementar detecção com base no aumento de um determinado percentual do número de transações por segundo (TPS);

2.2.6.58. Implementar detecção com base no aumento de carga e latência do servidor de aplicação;

2.2.6.59. Implementar detecção com base no número máximo de transações por segundo de um determinado IP;

2.2.6.60. Implementar mitigações para ataques DDoS, incluindo resolução de CAPTCHA, descarte de todas as requisições de um determinado IP, descarte por geolocalização IP, injeção de um desafio JavaScript para detectar se é um usuário legítimo ou bots;

2.2.6.61. Implementar mitigação de ataques DDoS através de assinaturas dinâmicas em tempo real para proteção da aplicação;

2.2.6.62. Implementar detecção e mitigação de ataques de força bruta de usuário/senha em páginas de login, com configuração da quantidade máxima de tentativas e tempo de mitigação; considerando:

I - Identificar ataques com diferentes usuários e mesma origem;

II - Identificar ataques com diferentes origens e mesmo usuário;

III - Identificar ataques de forma global, considerando a quantidade de tentativas e implementando contramedidas de forma global para a política. *contramedidas de forma global para a política.*

2.2.6.63. Suportar integração para consultas em listas externas, do próprio fabricante ou de terceiros, de credenciais expostas para mitigar ataques Credential Stuffing e Password Sprawl;

- 2.2.6.64. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs após validação sem sucesso de desafios e permitir a configuração do tempo de bloqueio;
- 2.2.6.65. Implementar mitigação através de listas de bloqueio dinâmica de endereços IPs que ultrapassem um número máximo de violações por minuto e permitir a configuração do tempo de bloqueio;
- 2.2.6.66. Implementar proteção de APIs através da imposição de regras de endpoint e métodos permitidos; considerando:
- I - Permitir a configuração de quotas e rate limits para chamadas em APIs de forma global na política;
 - II - Permitir a configuração de quotas e rate limits para chamadas em APIs por endpoint;
 - III - Permitir configurar exceções as regras de rate limits para chamadas na API;
- 2.2.6.67. Implementar proteção de conteúdo no formato JSON (JavaScript Object Notation);
- 2.2.6.68. Suportar proteção de conteúdo de mensagens no formato GraphQL, incluindo assinaturas de ataques, profundidade de query, GraphQL batching, inspeção de conteúdo JSON em mensagens POST e GET;
- 2.2.6.69. Suportar importação de especificação de API compatível com OpenAPI v2 e v3, nos formatos YAML ou JSON, com suporte a parâmetros no path e importação de respostas;
- 2.2.6.70. Implementar funcionalidade de autenticação e autorização de clientes de API utilizando, pelo menos, os métodos HTTP Basic e OAuth 2.0;
- 2.2.6.71. Implementar funcionalidade para prevenir vazamento de informações, dados sensíveis e outros tipos de dados confidenciais, sigilosos ou restrito, através do bloqueio ou remoção dos dados confidenciais;
- 2.2.6.72. Implementar funcionalidades para prevenir vazamento de dados sensíveis em mensagens de erro HTTP, códigos das aplicações, entre outros, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;
- 2.2.6.73. Implementar funcionalidade para ocultar erros de aplicação ou infraestrutura do usuário;
- 2.2.6.74. Permitir a configuração de fluxo de navegação da aplicação, de forma que um usuário só pode alcançar determinada URL se passar por outras anteriormente;
- 2.2.6.75. Permitir a correção de um falso positivo através da aceitação da requisição e atualização da política de forma automática;
- 2.2.6.76. Possuir um nível severidade de violação de múltiplos níveis para fácil identificação de violações de maior e menor prioridade;
- 2.2.6.77. Implementar um identificador único para cada requisição tratada pela solução;
- 2.2.6.78. Permitir o armazenamento local de eventos e exportação para servidores externos;
- 2.2.6.79. Permitir configurar a retenção dos eventos por tempo e volume;
- 2.2.6.80. Implementar a detecção, remoção ou codificação de dados sensíveis dos eventos como, por exemplo, números de cartão de crédito, CPF e senhas;
- 2.2.6.81. Implementar a criptografia de parâmetros específicos da aplicação, tais como credenciais e dados sensíveis, sem a necessidade de atualizar a aplicação. Esta criptografia de dados deve ser implementada no payload do HTTP, ou seja, nos dados propriamente ditos e não apenas via protocolo de transporte/túnel (TCP/TLS);
- 2.2.6.82. Implementar a ofuscação do nome de um parâmetro sensível da aplicação utilizando caracteres aleatórios, devendo ser mudado frequentemente pela solução para dificultar ataques direcionados;
- 2.2.6.83. Permitir exportar as políticas de segurança para arquivos texto, JSON ou XML;
- 2.2.6.84. Possuir integração com esteiras de automação que permita que as configurações sejam

realizadas de forma automática e dinâmica, de forma declarativa, por ferramentas de automação e orquestração, permitindo que a solução seja integrada ao ciclo de desenvolvimento;

2.2.6.85. Suportar integração nativa com funcionalidade de gestão avançada de tráfego automatizado para detecção e mitigação de ataques, abusos e fraudes, com detecção de tráfego gerado por usuários, bots benignos e malignos, através de telemetria de uso coletada da aplicação, sem a utilização de CAPTCHAs ou desafios para o navegador; considerando:

I - Suportar funcionalidade de forma nativa na solução ou possuir integração com serviço em nuvem do mesmo;

II - Suportar proteção de aplicações web, de dispositivos móveis e APIs;

2.2.6.86. A solução deve implementar a atualização das bases de inteligência de ameaças para proteção de aplicações web e API durante a vigência do contrato;

2.2.6.87. As fontes de inteligência devem ser fornecidas diretamente pelo fabricante da solução ou parceiros homologados através de assinaturas de serviços próprios, inclusas sem custo adicionais durante a vigência do contrato;

2.2.6.88. As fontes de inteligência devem ser atualizadas frequentemente pela duração do contrato sem custo adicional;

2.2.6.89. Deve dispor de bases de inteligência de IP, incluindo IPv4 e IPv6, classificados e categorizados em, pelo menos, as categorias fontes de ataques web, redes e hosts de botnets, scanners de websites, fontes de phishing, servidores proxies, redes e hosts que exploram vulnerabilidades em Windows, redes e hosts de negação de serviço e redes e hosts com baixa reputação;

2.2.6.90. Permitir que sejam criados filtros utilizando as categorias de IP nas funções de proteção de DDoS e serviços de DNS, de visibilidade de tráfego e de proteção de aplicações web e API;

2.2.6.91. Permitir utilizar a base de inteligência de IP durante consultas de DNS, permitir ações diferentes configuradas de acordo com a categoria e alterar a resposta antes de ser enviada para o cliente na solução de proteção de DDoS e serviços de DNS;

2.2.6.92. Permitir utilizar a base de inteligência de IP para classificar e selecionar uma cadeia de serviço na solução de visibilidade de tráfego;

2.2.6.93. Permitir que sejam criados filtros onde se verifica o endereço de origem no cabeçalho XForwarded-For (XFF) com base na classificação de endereços IP na solução de proteção de aplicações web e API;

2.2.6.94. Dispor de base de inteligência de ameaças relacionados a campanhas e ataques a aplicações web, correlacionando diversas fontes de inteligência e ameaças encontradas diariamente no mundo real; considerando:

I - As regras de proteção e assinaturas derivadas desta base de inteligência devem ser habilitadas automaticamente, sem precisar de um ciclo de aprendizagem na solução;

II - A base de inteligência deve implementar detecção e mitigação de ataques com baixo índice de falso-positivo;

III - Este serviço é complementar a atualização de assinaturas de ataques da solução de proteção de aplicações web e API, portanto, as informações disponibilizadas pela base de inteligência não devem ser limitada a apenas indicar qual assinatura do WAF for acionada, devendo disponibilizar informações contextuais incluindo, por exemplo, a capacidade de informar que um agente conhecido de ameaça usou uma exploração específica de vulnerabilidade mais recente (por exemplo, um CVE) em uma tentativa de implantação de uma ameaça como, por exemplo, um software de mineração de criptomoedas;

IV - As atualizações de regras devem ser automáticas e frequentes. As políticas, configurações e demais ajustes que dependem desta funcionalidade de inteligência devem ser atualizadas sem interrupção do serviço, sem necessidade de atualização do sistema operacional e nem reiniciar o equipamento a cada atualização.

2.3. CARACTERÍSTICAS ESPECÍFICAS DA SOLUÇÃO WAAP - Appliance Físico (item 1 do lote 1)

- 2.3.1. Possuir capacidade mínima para tratar 15 (quinze) Gbps de throughput em Camada 7;
- 2.3.2. Possuir capacidade mínima para tratar 24 (vinte e quatro) Gbps de throughput em Camada 4;
- 2.3.3. Possuir capacidade de compressão em Hardware de 14 (quatorze) Gbps;
- 2.3.4. Possuir capacidade de manter, no mínimo, 18.000.000 (dezoito milhões) de conexões simultâneas na camada 4;
- 2.3.5. Ter capacidade de receber 345.000(trezentos e quarente e cinco mil) novas conexões em camada 4 por segundo;
- 2.3.6. Possuir capacidade de processar 09 (nove) Gbps de throughput de tráfego SSL com chaves RSA de 2048 bits;
- 2.3.7. Processar 14.000 (quatorze mil) transações por segundo TLS com RSA 2K;
- 2.3.8. Processar 9.000 (nove mil) transações por segundo TLS com ECDHE-ECDSA P-256;
- 2.3.9. Possuir no mínimo 04 (quatro) interfaces 1/10G UTP RJ45;
- 2.3.10. Possuir no mínimo 04 (quatro) interfaces SFP+/SFP28 1/10/25G;
- 2.3.11. Possuir disco interno de 480GB com tecnologia SSD ou NVMe;
- 2.3.12. Possuir no mínimo 04 (quatro) interfaces 1/10G UTP RJ45;
- 2.3.13. Possuir no mínimo 04 (quatro) interfaces SFP+/SFP28 1/10/25G;
- 2.3.14. Ser fornecido com, no mínimo, 04 (quatro) transceivers 10GBASE-SR;
- 2.3.15. Possuir uma interface 1000BASE-T UTP RJ45 dedicada para gerenciamento;
- 2.3.16. Possuir uma interface USB 3.0 para transferência de arquivos;
- 2.3.17. Possui uma interface serial para gerenciamento;
- 2.3.18. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 2.3.19. Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;
- 2.3.20. Permitir configurar, pelo menos, 2.000 (duas mil) VLANs;
- 2.3.21. Possuir fontes internas redundantes;
- 2.3.22. Possuir altura máxima de 01 (um) RU e permitir instalação em rack padrão 19”;
- 2.3.23. A solução deve permanecer plenamente operante após o fim da garantia contratada, sem prazo determinado de funcionamento, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência.

2.4. CARACTERÍSTICAS ESPECÍFICAS DA SOLUÇÃO WAAP – Appliance|Virtual (item 2 do lote 1)

- 2.4.1. Possuir capacidade mínima para processar 900 (novecentos) Mbps de throughput;
- 2.4.2. Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;
- 2.4.3. A solução deve ser compatível com, no mínimo, as seguintes infraestruturas de virtualização e containerização:
 - a) Vmware vSphere;
 - b) Microsoft Hyper-V;

- c) KVM;
- d) Red Hat Open Shift.

2.4.4. A solução deve permanecer plenamente operante após o fim da garantia contratada, sem prazo determinado de funcionamento, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência.

2.5. **ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO WAAP SaaS**

2.5.1. Trata-se do fornecimento de serviço de proteção de aplicações Web e APIs em nuvem através de recursos integrados de segurança para mitigação de ataques distribuídos de negação de serviço (DDoS), gerenciamento e proteção de DNS, proteção contra (bots), firewall de aplicação web (WAF) e segurança de APIs, incluindo os serviços de instalação, comissionamento, testes, treinamento e gestão de conhecimento, consultoria, com suporte técnico e manutenção e garantia de hardware e software pelo prazo de 12 (doze) meses, no modelo SaaS.

2.5.2. **CARACTERÍSTICAS ESPECÍFICAS DA SOLUÇÃO WAAP SaaS - franquia de 2.5 TB/mês de tráfego limpo (item 4 do lote 1)**

2.5.2.1. **Administração, Gerenciamento e Monitoramento**

I - Os serviços devem ser prestados através de infraestrutura em nuvem do próprio fabricante da solução de forma não intrusiva, ou seja, sem a necessidade de instalação de equipamentos ou softwares nas dependências da CONTRATANTE;

II - O serviço em nuvem deverá ser oferecido em ponto(s) de presença em território nacional;

III - As atividades de administração, gerenciamento, operação e monitoramento dos serviços deverão ser através de console web única, gráfica e central do fabricante da solução, via HTTPS com algoritmos de criptografia modernos e seguros, compatível com navegadores padrões, não sendo aceitas soluções que dependam de plugins, add-ons ou aplicação exclusiva instaladas nas estações de trabalho;

IV - A console deve possuir controles de segurança, incluindo, mas não se limitando a, restrição de acesso administrativo por meio de um login seguro com autenticação de dois fatores de modo a prevenir que os serviços não sejam utilizados por terceiros não autorizados;

V - Permitir a criação de divisões administrativas de recursos através da criação de segmentos, partições, namespaces ou estrutura semelhante para agrupamento de recursos de diferentes propósitos, áreas ou finalidades da CONTRATANTE, tais como “Produção”, “Homologação” e “Desenvolvimento”, unidade de negócio, departamento, entre outros;

VI - Permitir a criação de usuários com acesso a console;

VII - Permitir a utilização de provedores de identidade para autenticação e autorização de usuários sem a necessidade de importar ou sincronizar com bases externas de usuários e senhas;

VIII - Implementar Single Sign-On (SSO) compatível com OpenID Connect (OIDC), tais como Okta, Microsoft, Google e outros;

IX - Permitir a configuração de Segundo Fator de Autenticação;

X - Permitir a criação de credenciais para acesso via API com data de expiração ou prazo de validade;

XI - Permitir definir políticas de senhas, incluindo tipos de caracteres, tamanho mínimo, validade e tentativas malsucedidas;

XII - Permitir a criação de grupos de usuários e associar usuários aos grupos;

XIII - Deve permitir a criação de perfis de acesso com diferentes níveis de acesso aos recursos da solução; considerando:

a) Dispor de diferentes perfis predefinidos com diferentes níveis de acesso para diferentes recursos da solução, incluindo acesso restrito, somente leitura, e leitura e escrita;

b) Permitir associar perfis de acesso a usuários por divisão administrativa;

c) Permitir associar perfis de acesso a grupos de usuários por divisão administrativa.

XIV - Implementar API REST autenticada através de tokens ou certificados para configuração de recursos, com documentação pública mantida pelo fornecedor do serviço; considerando:

a) Deve ser compatível com mTLS;

b) Dispor de um cliente de linha de comando (CLI) que implemente a API REST compatível com, pelo menos, Linux e Mac OS;

c) Possuir implementações específicas para ferramentas de automação no formato de provedores e módulos para Terraform ou coleções para Ansible.

XV - Permitir a exportação de eventos para sistemas externos, incluindo logs da solução e de requisições, segurança, e auditoria das aplicações;

a) Permitir a exportação para, pelo menos, os seguintes sistemas: Kafka, Splunk, Datadog, Azure, Amazon, QRadar e servidores HTTPS genéricos; considerando:

b) Permitir a configuração de, pelo menos, 02 (dois) destinos para envio de eventos.

XVI - Possuir painéis online para visualização de eventos e estatísticas, incluindo, no mínimo:

a) Saúde geral da aplicação;

b) Latência fim a fim;

c) Estatísticas de TLS;

d) Eventos com origem, destino, ataque e ação;

e) Taxas de requisições, status code e métodos;

f) Latência e throughput da aplicação;

g) Total de requisições ao longo do tempo;

h) Lista de aplicações e requisições, ataques e bloqueios;

i) Tipos de eventos;

j) Ataques, origens e alvos mais comuns;

k) Assinaturas e violações mais comuns;

l) Representação gráfica das API descobertas;

m) Taxa de requisições, resposta, códigos de resposta por endpoint da API;

n) Representação gráfica de interação entre endpoints da API;

o) Métodos, endpoints e eventos de segurança;

p) Sumário de segurança;

q) Classificação de bots das requisições;

r) Volume de requisições de bots e humanos;

s) Fluxos da aplicação mais atacados por bots;

- t) Lista de bots maliciosos por origem IP e tipo;
 - u) Informações de origem geográfica, dispositivos e plataformas relacionadas a bots;
 - v) Eventos de DDoS ao longo do tempo;
 - w) Taxa de requisições de ataques de DDoS;
 - x) Throughput do DDoS;
 - y) Mapa geográfico indicando a origem do DDoS;
 - z) Origens, regiões e ASN (Autonomous System Number) mais comuns relacionadas ao ataque de DDoS;
 - aa) Mapa geográfico das requisições de DNS por zona; ab) Gráfico de volume de requisições ao longo do tempo de DNS; ac) Lista de nomes de DNS mais solicitados;
 - ab) Lista de tipos de requisições de DNS mais solicitadas e gráfico ao longo do tempo;
 - ac) Gráfico de volume por tipo de resposta de DNS ao longo do tempo.
- XVII - Possuir relatório de incidentes de segurança para investigação de ataques com agrupamento automático de eventos em incidentes;
- XVIII - Permitir a configuração de agendamento de relatórios (diários, semanais ou mensais) e enviar os resultados por e-mail para usuários específico;
- XIX - Deve possuir Proteção contra DDoS, Firewall de Aplicação, Gerenciamento e Proteção de DNS, Mitigação de Bots.

2.5.2.2. **Proteção de Aplicações**

- I - Implementar serviço em nuvem, em infraestrutura própria do fabricante, de proteção de ataques a aplicações para proteção de websites, aplicações e APIs;
- II - Implementar gestão automática de certificados digitais, incluindo a renovação dos certificados, possuindo integração com, no mínimo, Let's Encrypt (<https://letsencrypt.org/>);
- III - Permitir a importação de certificado digital e chave privada da CONTRATANTE, devendo esta ser armazenada em repositório seguro e protegido;
- IV - Suportar OCSP;
- V - Permitir a configuração de múltiplos domínios (FQDN) para a mesma aplicação; considerando:
 - a) Suportar a gestão automática dos certificados de todos os domínios;
 - b) Permitir a importação de certificados digitais e chaves privadas de todos os domínios.
- VI - Permitir a configuração de diferentes conjuntos (pools) de servidores de origem da aplicação (Origin Servers) com algoritmos de balanceamento para escolha do pool;
- VII - Permitir configurar pesos e prioridades diferentes para cada Pool de Origin Servers;
- VIII - Permitir configurar um algoritmo de balanceamento de Origin Servers de um pool diferente do algoritmo de balanceamento de pools;
- IX - Permitir configurar monitores de disponibilidade de Origin Servers;
- X - Permitir a configuração de diferentes pools de Origin Servers selecionados a partir de atributos da aplicação, incluindo no mínimo método HTTP, prefixos expressões regulares da URL e cabeçalhos HTTP; considerando:
 - a) Permitir definir políticas de WAF diferentes por pool;
- XI - Permitir inserir cabeçalho HSTS (HTTP Strict-Transport-Security);

- XII - Implementar TLS 1.2 e superiores, com algoritmos fortes e cifras que suportem PFS (Perfect Forward Secrecy);
- XIII - Implementar Mutual TLS (mTLS) com a opção de enviar o certificado do cliente como cabeçalho HTTP para o Origin Server; considerando:
- Permitir especificar a lista de Autoridades Certificadoras (CA) de validação do certificado;
 - Permitir verificar o certificado do cliente em listas de revogação (CRL);
 - Permitir enviar o certificado completo;
 - Permitir enviar atributos específicos do certificado.
- XIV - Suportar HTTP/1.1 e HTTP/2;
- XV - Implementar inspeção e varredura com base em assinaturas para detecção de requisições maliciosas, incluindo, no mínimo proteções de:
- Cross-Site Scripting (XSS);
 - Cross-Site Request Forgery (CSRF);
 - Directory Traversal;
 - Directory Climbing;
 - SQL injection;
 - Cookie Injection;
 - Command Injection;
 - Code Injection;
 - Web Parameter Tampering;
 - Cookie Tampering.
- XVI - Implementar a configuração para identificação e mascaramento de dados sensíveis enviados pelo servidor para o cliente;
- XVII - Implementar detecção e mitigação de violações do protocolo HTTP;
- XVIII - Implementar proteção contra exploração de vulnerabilidade (exploit);
- XIX - Implementar proteção contra adulteração de cookies do serviço de proteção de aplicações;
- XX - Implementar inspeção, descoberta e proteção de requisições que utilizem GraphQL;
- XXI - Permitir a configuração de políticas de segurança de permissão e bloqueio;
- XXII - Permitir a criação de regras de exclusão de forma granular, considerando cookies, parâmetros, cabeçalhos e outros;
- XXIII - Permitir a configuração de políticas e regras que protejam as aplicações de ameaças e vulnerabilidades listadas no OWASP Top 10 e atualizações dessa lista;
- XXIV - Implementar proteções de campanhas de ataques e ameaças, informando a ação, o ator e a vulnerabilidade explorada;
- XXV - Permitir criar diferentes políticas de segurança para inspeção e proteção por aplicação;
- XXVI - Permitir habilitar uma política de segurança sem bloqueios, ou seja, apenas para geração de alertas ou monitoramento;
- XXVII - Implementar mecanismos de ajuste automático de assinaturas para redução de falso-positivos;

XXVIII

- Implementar fase de preparação de assinaturas de ataque, quando assinaturas novas e atualizadas são configuradas no modo de monitoramento por um período;

XXIX - Permitir desabilitar inspeções para tipos de ataques específicos;

XXX - Permitir definir os códigos de respostas HTTP (status code) que serão aceitos vindos da aplicação original, quando os demais códigos serão bloqueados;

XXXI - Permitir ocultar atributos e parâmetros sensíveis, tais como senhas ou outros dados sensíveis, em mensagens de log da plataforma;

XXXII - Permitir a criação de diferentes páginas de respostas de bloqueio, fornecendo um identificador de requisição;

XXXIII

- Permitir a criação de diferentes páginas de respostas por códigos de respostas HTTP (status code);

XXXIV

- Implementar a identificação de usuários e clientes a partir de informações extraídas de cabeçalhos IP. HTTP, parâmetros, cookies, JWT e fingerprint do TLS;

XXXV - Não serão aceitas soluções que classificam usuários apenas a partir do IP de origem;

XXXVI

- Implementar limitação de tráfego (rate limit) por usuário;

XXXVII

- Permitir a criação de regras de bloqueio com base na classificação do IP de origem e sua reputação; considerando:

a) Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas de ataques web;

XXXVIII

- Permitir a definição de taxa máxima de requisições (rate limit);

XXXIX

- Permitir definir uma lista de clientes confiáveis que não serão bloqueados por regras da política de segurança;

XL - Permitir definir uma lista de clientes suspeitos que devem ser bloqueados;

XLI - Implementar a inspeção com base no IP do cliente que iniciou a conexão e permitir utilizar o IP do cliente, o cabeçalho X-Forwarded-For por exemplo, presente no cabeçalho HTTP;

XLII - Permitir inserir cabeçalho HTTP na requisição e na resposta;

XLIII - Permitir remover cabeçalhos HTTP da requisição;

XLIV - Implementar o redirecionamento automático de HTTP para HTTPS;

XLV - Permitir a configuração de políticas de CORS (Cross-Origin Resource Sharing);

XLVI - Implementar mitigação automática de DDoS em camada 7;

XLVII - Implementar mitigação automática de ataques "Slow and low".

2.5.2.3. Proteção de APIs

I - A solução deve implementar descoberta automática de endpoints de API, proteção de DDoS em camada 7 e proteção de usuários maliciosos de API;

II - Deve ser totalmente integrado aos demais serviços, através da mesma console;

III - Implementar a validação de APIs através da importação de arquivos swagger

compatível com OpenAPI;

IV - Permitir importar diferentes versões de especificações de uma API;

V - Implementar a validação da API com base no arquivo swagger importado, permitindo que as ações de bloqueio, permissão e alerta seja criado para tráfego fora de conformidade; considerando:

a) Deve validar dados de entrada e saída, considerando o tipo de dados, comprimento mínimo e máximo, caracteres permitidos, intervalos de valores válidos;

b) Permitir a configuração de validação por endpoint da API, por grupos de API e com base no caminho;

c) Permitir configurar determinados IPs que não serão submetidos a validação.

VI - Implementar a validação de autenticação presente nas requisições de API, de acordo com o esquema de autenticação configurado de forma que somente clientes autenticados possam acessar a API;

VII - Permitir a configuração de proteções de APIs contra ameaças e vulnerabilidades listadas no OWASP API Security Top 10 e evoluções dessa lista;

VIII - Implementar a identificação por URL e método utilizado;

IX - Implementar a identificação e classificação de usuários. Entende-se por usuário como sendo um cliente identificado e classificado a partir de informações de endereço IP, de cabeçalhos, parâmetros e cookies do HTTP; considerando:

a) Não serão aceitas soluções que classificam usuários apenas a partir do IP de origem;

X - Implementar análise comportamental para detectar atividades anormais ou suspeitas a partir da análise do usuário, requisição e resposta;

XI - Implementar a detecção e mitigação de usuários maliciosos;

XII - Implementar análise da requisição e da resposta em busca de indícios de tráfego malicioso, abusos e vazamento de informações;

XIII - Permitir definir expressões para classificar informações e identificar possíveis vazamento de dados;

XIV - Permitir excluir URL do processo de descoberta;

XV - Implementar, a partir da descoberta, a construção automática do esquema (Swagger) da API;

XVI - Permitir documentar a descoberta de endpoints API;

XVII - Permitir agrupar as APIs descobertas para definição de políticas de segurança;

XVIII - Implementar regar de controle de API por endpoint, método e cliente;

XIX - Implementar políticas de controle de acesso da API a partir da descoberta;

XX - Implementar mecanismos para identificar “Shadow API”, ou seja, API que foram expostas pela aplicação, mas não foram aprovadas, documentadas ou homologadas;

XXI - Implementar mecanismos para identificar APIs zumbis, ou seja, que foram descobertas, mas não possuem atividade ou tráfego;

XXII - Permitir configurar a descoberta de API por aplicação;

XXIII - Permitir comparar o esquema definido da API com o que foi descoberto;

XXIV - Implementar detecção do tipo de autenticação utilizada na API e o local de utilização nas chamadas da API;

XXV - Implementar análise de vulnerabilidades da API, como dados sensíveis expostos, falta de autenticação, autenticação fraca, e fornecer nota de risco automática

calculada a partir das vulnerabilidades descobertas, impacto de ataque, impacto sobre o negócio, possibilidade de ataque e mitigação;

XXVI - Implementar proteção de ataques DDoS direcionados a API detectados a partir da análise comportamental;

XXVII - Implementar a descoberta e análise de cabeçalhos, conteúdo e assinaturas dentro dos campos de JSON Web Token (JWT), incluindo validação do algoritmo de assinatura, detecção de atributos do usuário e identificação de dados confidenciais.

2.5.2.4. **Proteção de Bots**

I - Implementar proteção de tráfego volumétrico de origem automatizada em aplicações web, dispositivos móveis e APIs;

II - Deve ser totalmente integrado aos demais serviços, através da mesma console;

III - Implementar a identificação por assinatura de bots para proteção de aplicações e APIs;

IV - Implementar a identificação através de análise de telemetria e indícios de automação;

V - Implementar a classificação de bots maliciosos e benignos, permitindo a resposta por classe de bot;

VI - Implementar resposta para requisições suspeitas de bots;

VII - Deve ser capaz de identificar scanners de vulnerabilidade, ferramentas de exploits e DoS, crawlers, spiders, assistentes de downloads, motores de buscas e de redes sociais;

VIII - Deve ser capaz de identificar e classificar ações automatizadas por bots maliciosos, bots benignos e usuários humanos;

IX - Implementar mecanismos para detectar técnicas avançadas e sofisticadas de automação, tais como click-farms, agentes humanos, emuladores e simuladores, “macro runners” e implementar mitigação;

X - Implementar mecanismos de análises adaptativas de comportamentos e uso das aplicações e implementar mitigação;

XI - Deve suportar integração com diversos fluxos da aplicação, tais como login, criação de contas, recuperação de senha, recuperação de contas, assinaturas de newsletter, entre outros; considerando:

a) Permitir classificar os fluxos protegidos de proteção, tais como login, gestão da conta, reset de senha e outros para geração de relatórios;

XII - A solução não deve armazenar e processar dados pessoais, credenciais, dados digitados, payload, arquivos e informações que permitem a identificação pessoal. Será admitida a coleta e processamento do endereço IP, cabeçalhos e suas informações relacionadas, assim como o registro de utilização de teclas/caracteres;

XIII - Deve ser capaz de detectar e mitigar ataques de credential stuffing, account takeover, content scrapers, carding fraud, marketing fraud e inventory hoarding;

XIV - Deve ser capaz de detectar acesso provenientes de bots e classificar os tipos de automação utilizados;

XV - Não serão aceitas soluções que dependem principalmente de CAPTCHAs para detecção e mitigação;

XVI - Não serão aceitas soluções que dependem principalmente de desafios em JavaScript para o navegador para detecção e mitigação;

XVII - Para aplicações web:

- a) Permitir a inserção do código JavaScript nas páginas da aplicação;
- b) Permitir especificar páginas que não devem receber a inserção do JavaScript;
- c) Implementar a coleta de telemetria de aplicações web relacionados ao acesso e rede, ambiente e navegador, e ao comportamento e o modo de uso da aplicação no navegador e webview;
- d) Implementar ofuscação avançada do código para prevenir técnicas de engenharia reversa;
- e) Implementar atualizações/rotação do código de extração de telemetria de forma automática e frequente para dificultar a ações de engenharia reversa;
- f) Implementar técnicas contra tentativas de análises da telemetria coletados;
- g) Não serão admitidas soluções que utilizam códigos JavaScript de fácil leitura;
- h) Não serão admitidas soluções que utilizam telemetria coletados de fácil leitura.

XVIII - Para aplicativos para dispositivos móveis:

- a) Implementar coleta de telemetria relacionados ao acesso e rede, ambiente e dispositivo, e ao comportamento e modo de uso do aplicativo nativo para dispositivos móveis através de SDK incorporado ao aplicativo;
- b) Deve ser totalmente compatível com as políticas de publicações de aplicativos das lojas Apple App Store e Google Play Store;
- c) Ser compatível com aplicativos Android na versão 5.x e superior (API Level 21) e aplicativos para iOS na versão 9.x e superior;
- d) Suportar frameworks estáticos e dinâmicos de aplicativos para dispositivos móveis, tais como React, Flutter, Angular e Ionic;
- e) A atualização das políticas de coletas de telemetria não deve exigir a redistribuição ou atualização dos aplicativos nos dispositivos móveis.

XIX - Deve apresentar o resultado da análise da telemetria de forma determinística, ou seja, através de um veredito simples se se trata de tráfego automatizado, indicando, quando disponível, o motivo ou tipo de automação detectado.

2.5.2.5. **Mitigação de Ataques Distribuídos de Negação de Serviço (DDoS)**

- I - Implementar defesa automática de ataques de Distributed Denial-Of-Service (DDoS), protegendo continuamente todas as aplicações publicadas através do serviço contratado em nuvem;
- II - Deve mitigar ataques de forma transparente para a aplicação, absorvendo e bloqueando ataques;
- III - Deve ser capaz de detectar ataques através da análise das taxas de requisição, erros, latência e throughput da aplicação;
- IV - Implementar proteção de ataques na camada de aplicação, incluindo os protocolos HTTP e DNS, incluindo, no mínimo, proteções de HTTP GET Flood, HTTP POST Flood, Slowloris e DNS Flood;
- V - Implementar proteção de ataques volumétricos, incluindo SYN Flood, UDP Flood, TCP Flood e ICMP Flood;
- VI - Implementar proteção de ataques de negação de serviço através da exaustão de recursos (“Slow DDoS”), incluindo Slow POST e Slowloris;
- VII - Implementar proteção de ataques à pilha TCP;
- VIII - Implementar proteção de ataques que utilizam falsificação de endereços IP de origem (IP spoofing);

- IX - Implementar detecção e mitigação automática de ataques em Camada 7 em larga escala;
- X - Implementar proteção através de bloqueio geográfico e de, pelo menos, 100 (cem) prefixos IP;
- XI - Permitir criar regras de bloqueio personalizadas;
- XII - Permitir configurar o bloqueio de clientes com base no TLS fingerprint;
- XIII - Permitir configurar o bloqueio de clientes com base na classificação e reputação do IP; considerando:
 - a) Deve possuir, pelo menos, a classificação de IP para botnets, scanners, proxies anônimos, proxies ToR e origens conhecidas por ataques web;
- XIV - Permitir configurar o bloqueio de clientes com base no ASN do BGP;
- XV - Permitir configurar de mitigações específicas por aplicação;
- XVI - Permitir configurar rate limit por aplicação;
- XVII - Permitir configurar rate limit por usuário, onde entende-se por usuário como sendo um cliente da aplicação identificado por um IP de origem, um cookie, um cabeçalho, parâmetro da query, fingerprint TLS, geolocalização, ou combinação de alguns desses.

2.5.2.6. Gerenciamento e Proteção de DNS

- I - Implementar serviço DNS primário e secundário;
- II - Implementar zona de pesquisa direta (Forward DNS Lookup Zone) e reverso (Reverse Lookup Zone);
- III - Para as zonas hospedadas na solução, implementar a configuração automática de domínios e FQDN utilizados nas aplicações publicadas pela solução;
- IV - Possuir interface gráfica para gerenciamento de registros do DNS;
- V - Implementar DNSSEC (Domain Name System Security Extensions) com gerenciamento automático de chaves;
- VI - Implementar proteções de ataques direcionados aos serviços de DNS;
- VII - Implementar proteções de ataques de DDoS;
- VIII - Implementar a configuração de registros de DNS para funcionalidade de balanceamento de sites (Global Server Load Balancer – GSLB); considerando:
 - a) Implementar a verificação de disponibilidade dos sites através de testes HTTP e
 - b) ICMP;
 - c) Implementar, pelo menos, os algoritmos de balanceamento round robin, prioridade, peso e origem;
 - d) Implementar persistência da resolução de nomes utilizando, pelo menos, o Local DNS da requisição;
 - e) Permitir configurar topologias para respostas com base em geolocalização.

2.5.2.7. Recursos Disponíveis por Unidade do Serviço de Proteção em Nuvem

- I - Configuração de até 05 (cinco) load balancers, cada um capaz de suporta até 05 (cinco) aplicações, com um total de até 150 (cento e cinquenta) Origin Servers e com franquia de 2,5 (dois vírgula cinco) TB por mês de volume de transferência de dados sem considerar tráfego de ataques;
 - a) Entende-se por aplicação como a configuração de um FQDN ou domínio que deve

ser protegido por uma política de segurança, acessível através da infraestrutura em nuvem por um IP ou CNAME, independentemente da quantidade de paths ou URL deste FQDN;

II - Capacidade de limitar taxas de requisições válidas (rate limit) de usuários identificados de, no mínimo, 500.000 (quinhentas mil) requisições/dia entre todas as aplicações;

III - Capacidade de descobrir as APIs em, no mínimo, 05 (cinco) load balancers, incluindo até 05 (cinco) aplicações em cada LB, independentemente da quantidade de requisições/dia;

IV - Capacidade de proteger as APIs de, no mínimo, 150.000 (cento e cinquenta mil) requisições/dia válidas entre todas as aplicações;

V - Capacidade de proteção de bots de, no mínimo, 500.000 (quinhentas mil) transações/dia entre todas as aplicações;

VI - Capacidade de mitigar DDoS direcionado as aplicações protegidas independente do volume de tráfego, sem custo adicional;

VII - Serviço de DNS autoritativo primário e secundário para, no mínimo, 200 (duzentas) zonas, sem limite de resoluções e resposta de DNS;

VIII - Serviço de balanceamento de DNS para, pelo menos 30 (trinta) endereços IP; IX - Garantir via console o acesso, busca e consulta de eventos por, no mínimo:

a) 30 (trinta) dias para métricas de desempenho e eventos de auditoria;

b) 07 (sete) dias para eventos de requisições e segurança;

c) Para eventos mais antigos, a solução deve garantir o armazenamento de, pelo menos, 50 (cinquenta) GB de mensagens ou manter os eventos por até 30 dias.

2.5.3. **Franquia Adicional de Tráfego Limpo - WAAP SaaS (item 5 do lote 1)**

I - Será oferecida uma franquia adicional de volume de tráfego excedente, pelo período do contrato, a ser consumido após o esgotamento do tráfego mensal contratado;

II - A menor fração de tráfego adicional será de 1 TB (Um Terabyte);

III - O painel de monitoramento deverá permitir a mensuração e controle em tempo real da utilização de tráfego eventualmente transportado. A ferramenta deverá possibilitar a emissão de relatórios gerenciais com quantitativos e consumos por período.

3. **ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DO LOTE 2**

3.1. Contratação de empresa do ramo de Tecnologia da Informação para o fornecimento de solução Application Delivery Controller – ADC em modalidade aquisição perpétua de hardware e software, com garantia de 36 meses, com instalação/configuração, suporte técnico e treinamento da solução.

3.2. **ESPECIFICAÇÕES GERAIS DO APPLIANCE ADC/LOAD BALANCE (item 1 do lote 2)**

3.2.1. Possuir capacidade mínima para tratar 9 (nove) Gbps de throughput em Camada 7;

3.2.2. Possuir capacidade mínima para tratar 9 (nove) Gbps de throughput em Camada 4;

3.2.3. Possuir capacidade de manter, no mínimo, 30.000.000 (trinta milhões) de conexões simultâneas na camada 4;

3.2.4. Ter capacidade de tratar 500.000 (quinhentas mil) novas conexões em camada 4 por segundo;

- 3.2.5. Ter capacidade de tratar 180.000 (cento e oitenta mil) requisições em camada 7 por segundo;
- 3.2.6. Possuir capacidade de processar 8 (oito) Gbps de throughput de tráfego SSL com chaves RSA de 2048 bits;
- 3.2.7. Processar 10.000 (dez mil) transações por segundo TLS com RSA 2K;
- 3.2.8. Processar 5.000 (cinco mil) transações por segundo TLS com ECDHE-ECDSA P-256;
- 3.2.9. Possuir no mínimo 07 (sete) interfaces 1G UTP RJ45;
- 3.2.10. Possuir no mínimo 04 (quatro) interfaces SFP+ 1/10G e cada unidade de equipamento, deverá ser fornecida com seus respectivos transceivers do tipo 10GBASE-SR;
- 3.2.11. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
- 3.2.12. Suportar 802.1q para o transporte de múltiplas VLAN por uma única porta e por um conjunto agregado de portas;
- 3.2.13. Permitir configurar, pelo menos, 2.000 (duas mil) VLANs;
- 3.2.14. Possuir disco interno com tecnologia SSD ou NVMe;
- 3.2.15. Possuir altura máxima de 01 (um) RU e permitir instalação em rack padrão 19”;
- 3.2.16. A solução deve permanecer plenamente operante após o fim da garantia contratada, sem prazo determinado de funcionamento, sem interrupção de tráfego ou funcionalidades, sendo admitido apenas o encerramento dos serviços de atualização de assinaturas e bases de inteligência.

3.2.17. **Hardware**

- 3.2.17.1. Equipamentos fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas neste caderno de especificações técnicas;
- 3.2.17.2. Suportar quantidade de memória e capacidade de processamento suficiente para o atendimento de todas as funcionalidades e desempenho solicitados neste documento;
- 3.2.17.3. Fontes de alimentação Full Range, operando na faixa de tensões de 100 a 240 Vac e frequência de 60Hz;
- 3.2.17.4. Compatível para montagem em rack padrão de 19 (dezenove) polegadas, incluindo todos os acessórios necessários ao seu pleno funcionamento;
- 3.2.17.5. Fornecido com todos os cabos de ligação lógica e elétrica necessários à instalação e perfeito funcionamento;
- 3.2.17.6. Serem novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não podem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie;
- 3.2.17.7. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;
- 3.2.17.8. Vir acompanhado de todas as licenças de software ou hardware necessárias para atendimento das funcionalidades exigidas neste caderno de especificações técnicas;
- 3.2.17.9. Todas as funcionalidades devem continuar ativas, mesmo após o término do termo de garantia e suporte técnico.

3.2.18. **Conectividade;**

- 3.2.18.1. A CONTRATADA, mediante demanda, fará a interligação das interfaces com os switches da rede junto com a CONTRATANTE;
- 3.2.18.2. Todas as interfaces fornecidas podem estar licenciadas e habilitadas para uso imediato;

- 3.2.18.3. Possuir suporte a IPv4 e IPv6;
- 3.2.18.4. Implementar a norma IEEE 802.1q para marcação de VLANs;
- 3.2.18.5. Suportar sub-interfaces ethernet lógicas;
- 3.2.18.6. Permitir agregação de interfaces baseado no protocolo LACP segundo o padrão IEEE 802.3ad comportando no mínimo 8 (oito) interfaces;
- 3.2.18.7. Implementar os seguintes padrões e protocolos de STP (Spanning Tree Protocol): IEEE 802.1d — MAC Bridges, IEEE 802.1s — Multiple Spanning Trees e IEEE 802.1w — Rapid Reconfiguration of Spanning Tree; ou ter a capacidade de tornar-se transparente às BPDUs encaminhadas pelos equipamentos de rede conectados a essa solução;
- 3.2.18.8. Suportar VXLAN;
- 3.2.18.9. Suportar NVGRE;
- 3.2.18.10. Implementar Access Control Lists (ACLs);
- 3.2.18.11. Permitir o encaminhamento de “jumbo frames” (pacotes de 9016 bytes) em todas as interfaces utilizadas para tráfego de dados.

3.2.19. **Roteamento Avançado**

- 3.2.19.1. Permitir a criação de rotas estáticas e suportar, no mínimo, os protocolos de roteamento dinâmico OSPF, BGP e RIP;
- 3.2.19.2. Suportar roteamento dinâmico para IPv4 e IPv6 (OSPF, BGP);
- 3.2.19.3. Suportar roteamento estático de tráfego IPv6 e IPv4.
- 3.2.19.4. A solução deve suportar os seguintes protocolos de roteamento BGP, OSPF e RIP em IPv4 e IPv6;
- 3.2.19.5. Implementar Policy Based Routing e Policy-Based Forwarding.
- 3.2.19.6. Suportar Equal Cost Multipath (ECMP);
- 3.2.19.7. Implementar endereçamento IPv6;
- 3.2.19.8. Permitir a configuração de endereços IPv6 para gerenciamento.
- 3.2.19.9. Implementar ICMPv6;
- 3.2.19.10. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6;
- 3.2.19.11. Implementar listas de controle de acesso (ACLs) em IPv6;
- 3.2.19.12. Permitir a configuração de Virtual IP Address (VIPs), servidores reais e probes em IPv6.
- 3.2.19.13. Implementar o roteamento IPv6 em pelo menos os seguintes cenários:
- 3.2.19.14. 3.Suportar roteamento estático para IPv6;
- 3.2.19.15. 3Suportar protocolo de roteamento dinâmico OSPFv3;
- 3.2.19.16. Implementar roteamento dinâmico RIPng;
- 3.2.19.17. Implementar roteamento dinâmico IS-IS V4/V6.

3.2.20. **Requisitos de Gerenciamento**

- 3.2.20.1. Possuir no mínimo 1 (uma) porta de console para administração local do equipamento;
- 3.2.20.2. Ter suporte a sFlow;
- 3.2.20.3. Ter suporte a netFlow v9 and v10 (IPFIX);
- 3.2.20.4. O equipamento deve ser gerenciável através de protocolo SNMP v2c e v3 e ainda pode

possuir suporte a MIB II;

- 3.2.20.5. Permitir a autenticação de usuários (switch log on), através de RADIUS ou TACACS+, implementando AAA (autorização, autenticação e contabilização);
- 3.2.20.6. Implementar controle de acesso baseado em regras configuráveis (Role Based Access Control – RBAC);
- 3.2.20.7. Implementar acesso à interface de linha de comando via protocolo SSH para gerenciamento;
- 3.2.20.8. Implementar acesso a interface gráfica via web para gerenciamento;
- 3.2.20.9. A interface Gráfica deve permitir a reinicialização do equipamento;
- 3.2.20.10. Reinicialização do equipamento por comando na CLI;
- 3.2.20.11. Possuir capacidade de armazenamento de logs de auditoria, para registro de todas as atividades dos usuários da ferramenta;
- 3.2.20.12. Implementar Debugging: CLI via console e SSH;
- 3.2.20.13. Permitir a gravação de eventos em registro interno (log) e externo (syslog);
- 3.2.20.14. Ser capaz de realizar notificações de eventos de segurança através de email, traps SNMP e Syslog.

3.2.21. **Alta disponibilidade**

- 3.2.21.1. Suportar e garantir a instalação em ambiente de alta disponibilidade;
- 3.2.21.2. Permitir a configuração da solução em alta disponibilidade, permitindo o funcionamento em cluster do tipo ativo-passivo e ativo-ativo;
- 3.2.21.3. A solução deve suportar mais do que dois elementos no cluster para sincronização de configuração de forma nativa a fim de permitir escalabilidade no futuro;
- 3.2.21.4. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades;
- 3.2.21.5. Possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência;
- 3.2.21.6. O equipamento deve permitir a sincronização das configurações de forma automática;
- 3.2.21.7. A configuração dos equipamentos de ser baseada em perfis, permitindo fácil administração;
- 3.2.21.8. Os perfis podem ser hierarquizados, permitindo maior facilidade na administração de políticas similares.

3.2.22. **Requisitos de balanceamento local de servidores (SLB)**

- 3.2.22.1. Permite implementar todas as funcionalidades comuns de um Switch camada 7:
 - I - Server Load-Balancing;
 - II - Firewall Load-Balancing;
 - III - Proxy Load-Balancing;
 - IV - Global Site Load-Balancing;
 - V - Transparent Cache Switch;
 - VI - URL Switching; VII - Inserção de Cookies; VIII - Cookie Switching.
- 3.2.22.2. Permitir implementar a otimização do protocolo TCP para ajustes de parâmetros das conexões cliente e servidor;

- 3.2.22.3. Possuir suporte para multiplexação de conexões nos servidores usando o protocolo HTTP 1.1, ou seja, pode ser capaz de abrir um número específico de conexões TCP com o servidor e inserir todos os HTTP requests gerados pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço;
- 3.2.22.4. Ser capaz de fazer log de todas as sessões, onde os registros podem conter:
- I - Endereço IP de origem;
 - II - Porta TCP ou UDP de origem;
 - III - Endereço IP de destino;
 - IV - Porta TCP ou UDP de destino;
 - V - Data e hora da mensagem;
 - VI - URL acessada;
 - VII - Cookie utilizado.
- 3.2.22.5. Pode ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente;
- 3.2.22.6. Pode permitir compressão tipo GZIP;
- 3.2.22.7. Pode ser possível definir compressão especificamente para certos tipos de objetos;
- 3.2.22.8. O equipamento pode tratar o balanceamento de tráfego com base, pelo menos, nos seguintes protocolos:
- I - TCP, UDP;
 - II - HTTP, HTTPS;
 - III - FTP.
- 3.2.22.9. O equipamento deve prover as funcionalidades de balanceamento de tráfego baseado em regras customizáveis de camada 4 e 7 do modelo ISO/OSI;
- 3.2.22.10. O equipamento deve suportar o uso de expressões regulares para modelar políticas (regras) de balanceamento baseados em URL, cookies e campos do cabeçalho HTTP;
- 3.2.22.11. O equipamento deve suportar qualquer formato de URL e cookies, permitindo o balanceamento de um website sem alteração de formato da URL ou cookies;
- 3.2.22.12. O equipamento deve suportar o balanceamento quando as VLANs do lado cliente e do lado servidor estiverem tanto na mesma VLAN, quanto em VLAN diferente;
- 3.2.22.13. Implementar balanceamento L7 em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente.
- 3.2.22.14. O equipamento deve suportar, no mínimo, os seguintes métodos de balanceamento:
- I - Round Robin;
 - II - Round Robin ponderado;
 - III - Least Connections;
 - IV - Least Connections ponderado;
 - V - Tempo de Resposta do Servidor.
- 3.2.22.15. Suportar a utilização de endereço IPv6 tanto pelos servidores quanto pelos clientes;
- 3.2.22.16. Deve suportar monitoração da disponibilidade dos Servidores;
- 3.2.22.17. O equipamento deve, mediante demanda, suportar a monitoração contínua da disponibilidade das aplicações e dos servidores balanceados a partir de testes (probes) para a monitoração do estado dos servidores/aplicações, com base na avaliação do código de retorno;
- 3.2.22.18. Na ocorrência de falha em servidores reais (ou de gateways do balanceamento) detectada

pela monitoração, o balanceador pode retirar o servidor deficitário do pool e redirecionar o tráfego para outros servidores do mesmo pool ou para outro pool de servidores;

3.2.22.19. Quando o teste detectar que a falha não mais ocorre, o balanceador pode automaticamente recolocar o servidor operacional no pool, de forma dinâmica, sem interrupção do serviço do balanceamento do mesmo pool;

3.2.22.20. Implementar os seguintes métodos de monitoramento dos servidores reais, de forma nativa ou por meio do uso de monitores personalizados:

- I - Layer 3 - ICMP;
- II - Layer 4 - Conexões TCP e UDP pela porta respectiva no servidor;
- III - Layer 7 - Verificação específica ao protocolo de aplicação, suportando, no mínimo: HTTP, HTTPS, FTP, SMTP, MSSQL, LDAP, IMAP, POP3, SIP, DNS, SNMP;
- IV - Implementar método de monitoramento dos servidores reais personalizados por meio de scripts.

3.2.22.21. Persistência de Sessão do Usuário:

- I - O equipamento suporta persistência de sessão de usuário, permitindo que todas as conexões de uma sessão cliente sejam tratadas pelo mesmo servidor, a fim de que as sessões estabelecidas não sejam interrompidas.

3.2.22.22. O equipamento deve suportar os seguintes mecanismos de persistência:

- I - por cookie - método cookie insert e cookie rewrite;
- II - por endereço IP origem;
- III - por endereço IP destino;
- IV - por sessão SSL;
- V - analisando a URL acessada;
- VI - analisando a URL e cookie concorrentemente;
- VII - analisando qualquer parâmetro no header HTTP.

3.2.23. **Requisitos de Balanceamento Global**

3.2.23.1. A solução deve possuir o recurso de balanceamento de tráfego através de múltiplos sites físicos;

3.2.23.2. A solução deve monitorar o estado dos balanceadores em sites remotos, no mínimo nos seguintes parâmetros:

- I - (1) Tempo de resposta dos servidores;
- II - (2) Uso da CPU;
- III - (3) Disponibilidade e uso de sessões.

3.2.23.3. Implementar as seguintes funcionalidades de balanceamento global (GSLB):

- I - Round Robin;
- II - Disponibilidade e carga da aplicação (site load);
- III - Weighted round robin;
- IV - Least Connection; e,
- V - De acordo com a localidade (geo-localização).

3.2.23.4. Permitir a parametrização de um limite máximo de conexões por servidores reais, ou por VIP (Virtual IP), quando for necessário nas configurações de balanceamento.

3.2.24. **Requisitos de Virtualização / Particionamento**

- 3.2.24.1. Deve ser capaz de implementar, no mínimo, 32 (trinta e duas) instâncias (partições) de gerenciamento com isolamento de tráfego, onde cada instância pode ter sua própria tabela de roteamento;
- 3.2.24.2. Cada instância deve possibilitar o uso de todas as funcionalidades adquiridas;
- 3.2.24.3. Permitir a definição de limites de conexão, banda, requisições, interfaces de rede, entre outros – para as instâncias;
- 3.2.24.4. Permitir a configuração e gerenciamento das instâncias de forma isolada e independente das demais, isto é, sem gerar indisponibilidade ou influência negativa no desempenho.

3.2.25. **Redirecionamento**

- 3.2.25.1. A solução deve possuir redirecionamento global baseada nos seguintes métodos: DNS, HTTP e Proxy (NAT dos clientes) para as aplicações que não usem DNS nem sejam HTTP;
- 3.2.25.2. O redirecionamento global através de DNS Pode suportar a resolução de registros DNS de tipo A, AAAA e PTR;
- 3.2.25.3. A solução pode suportar DNS queries em IPv4 e IPv6;
- 3.2.25.4. O redirecionamento DNS Pode suportar DNSSEC;
- 3.2.25.5. O redirecionamento DNS Pode suportar DNSSEC Key Rollover de acordo à RFC 4641;
- 3.2.25.6. A solução deve fornecer persistência na seleção do site via DNS;
- 3.2.25.7. Requisitos de compressão:
 - I - A solução deve suportar compressão HTTP;
 - II - Utilizar os algoritmos de compressão Gzip;
 - III - Pode ser possível definir compressão especificamente para certos tipos de objetos com o objetivo de diminuir a quantidade de informações enviadas para os clientes.

3.2.26. **Proxy Reverso**

- 3.2.26.1. Possuir função de atuar como proxy reverso para as aplicações web balanceadas permitindo no mínimo:
- 3.2.26.2. Redirecionamento de requisições para diferentes grupos de servidores, de acordo com qualquer parâmetro da requisição;
- 3.2.26.3. Alteração da resposta a ser enviada ao requisitante de acordo a qualquer parâmetro da resposta do servidor;
- 3.2.26.4. Apresentar página ao cliente em caso de total indisponibilidade do serviço web requisitado;
- 3.2.26.5. Redirecionamento do tráfego a um grupo de servidores backup em caso de indisponibilidade do grupo principal.

3.2.27. **Camada de Gerência Centralizada**

- 3.2.27.1. Será admitida a possibilidade de entrega do gerenciamento centralizado em sistema dedicado. Neste caso, deve ser fornecido em appliance virtual, compatível com “hypervisor” baseado em VMware, ou baseado em software, compatível com as versões vigentes dos sistemas CentOS e Red Hat Enterprise Linux;
- 3.2.27.2. Na hipótese do fornecimento de appliance virtual referido no item anterior, a infraestrutura de virtualização será de responsabilidade do Contratante;
- 3.2.27.3. Deve ser capaz de gerenciar de forma centralizada tanto dispositivos físicos, virtuais e instâncias (ou partições);

- 3.2.27.4. Possibilitar o acesso a todas as MIBs dos equipamentos ofertados, inclusive proprietárias, fornecendo todas as mídias e licenças necessárias ao pleno funcionamento de todas as funcionalidades exigidas;
- 3.2.27.5. Permitir visualização gráfica em tempo real do status dos equipamentos fornecidos quanto as interfaces, redundância e servidores virtuais, bem como dos resultados dos testes executados pelas probes nos servidores balanceados;
- 3.2.27.6. Fornecer funcionalidades necessárias para monitoração, avaliação da solução, assim como, a geração de estatísticas, relatórios, alarmes e eventos;
- 3.2.27.7. Ter capacidade de geração e exportação de relatórios, customizados por hora, dia, semana e mês, contendo informações sobre inventário de equipamentos, utilização de recursos de CPU, memória, interfaces de rede, servidores virtuais ("virtual server"), "pool" de servidores e os maiores demandadores de recursos (top-users);
- 3.2.27.8. Permitir a configuração de limites ("thresholds") para os parâmetros monitorados de maneira a gerar alarmes sempre que um limite for ultrapassado;
- 3.2.27.9. O sistema de gerenciamento deve manter registros de eventos e alertas classificados por criticidade;
- 3.2.27.10. Permitir a configuração de alertas que informem automaticamente sobre ataques e anomalia de tráfego, através de "thresholds" baseados na "baseline" da rede ou através de limites de tráfego atingido;
- 3.2.27.11. Permitir o registro de informações sobre indicadores de falhas, de desempenho, de mudanças de configuração dos dispositivos gerenciados, através de log de eventos;
- 3.2.27.12. Permitir a monitoração de indicadores de desempenho dos equipamentos gerenciados por meio de apresentação gráfica ("dashboards") da utilização de CPU, memória, interfaces de rede, servidores virtuais ("virtual server"), "pool" de servidores e aplicações;
- 3.2.27.13. As informações coletadas devem permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pelo balanceador;
- 3.2.27.14. Prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões (número de conexões TCP).
- 3.2.27.15. Possuir a capacidade de programação por meio de linguagem script e automatização dos dispositivos gerenciados através de API (Interface de programação de aplicações) compatível com o Appliance;
- 3.2.27.16. A solução deve processar as informações coletadas dos dispositivos gerenciados para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações;
- 3.2.27.17. Permitir a análise das aplicações que fazem uso de tráfego SSL/TLS criptografado;
- 3.2.27.18. Possuir capacidade de armazenamento de logs de auditoria, para registro de todas as atividades dos usuários da ferramenta;
- 3.2.27.19. Permitir a realização e alteração das configurações dos elementos gerenciados remotamente;
- 3.2.27.20. Ser capaz de exibir, permitir edição, upload e download das configurações, em formato texto, dos dispositivos geridos;
- 3.2.27.21. Ser capaz de realizar o processo de "backup" e "restore" dos arquivos de configuração dos equipamentos gerenciados;
- 3.2.27.22. Permitir alterações de configuração das funcionalidades de balanceamento dos elementos gerenciados de forma remota;
- 3.2.27.23. Permitir autenticação, autorização e contabilização (AAA) no acesso de usuários à console de gerência dos equipamentos, utilizando os métodos:

- I - Deve suportar autenticação de usuário/senha locais, Radius ou Tacacs/Tacacs+;
- II - Implementar controle de acesso baseado em regras configuráveis (Role Based Access Control – RBAC);
- III - Permitir a criação de grupos de usuários com perfis diferenciados, como por exemplo, de administrador, operador e outros, com níveis diferenciados de permissões de criar, definir, editar e gerenciar todos os equipamentos cadastrados.

3.2.27.24. Permitir a segmentação da gerência, de modo que os administradores de cada CCD (CS e SPM) tenham acesso somente aos equipamentos do seu CCD. Os demais equipamentos poderão ser exibidos, mas podem aparecer como desabilitados para administradores não autorizados;

3.2.27.25. Suportar comunicação com os protocolos NTP ou SNTP;

3.2.27.26. Ser ofertado com a versão mais recente (última versão disponível) do software de gerência;

3.2.27.27. Não pode haver licença restringindo o número de administradores que poderão ter acesso à Gerência Centralizada, seja por acesso via WEB ou por software cliente específico.



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:08, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112343713** e o código CRC **1581BEA2**.



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 TERMO DE REFERÊNCIA

MODELO DE RELATÓRIO DE CUMPRIMENTO DO OBJETO

obs: Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

(logo da empresa)

1. IDENTIFICAÇÃO			
Contrato nº			
Contratada		CNPJ	
nº da OS/OF		Período de Referência	

2. ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES DE ENTREGA/EXECUÇÃO					
Descrição do Objeto Contratado					
Item / Lote	Descrição do bem ou serviço	Métrica	Quantidade	Valor Unitário	Valor Total
Valor Total					

3. OBSERVAÇÕES

4. ENCAMINHAMENTO

Por este instrumento, encaminhamos as informações e documentos comprobatórios dos serviços correspondentes à [Ordem de Serviço ou de Fornecimento] acima identificada, conforme definido no Modelo de Execução do contrato supracitado, para que seja verificado o devido cumprimento dos requisitos e demais condições contratuais

5. PREPOSTO

Nome
CPF

Local e Data



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:09, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112343334** e o código CRC **36D4D00B**.



Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO III DO TERMO DE REFERÊNCIA

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

ANEXO XXX - DO CONTRATO

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

Eu, <nome completo>, <ocupação institucional>, <órgão público / entidade>, <matrícula>, <CPF>, declaro a ciência das obrigações e responsabilidades decorrentes do tratamento de dados pessoais realizado durante a vigência contratual, observando o integral teor do presente Termo de Responsabilidade.

Considerando as obrigações a mim conferidas, no bojo deste Termo de Responsabilidade, comprometo-me a:

- a) manusear as bases de dados com objetivo exclusivo de alcançar a finalidade específica atrelada ao tratamento dos dados pessoais envolvidos;
- b) não compartilhar com terceiros os dados pessoais sujeitos a qualquer espécie de tratamento, salvo se por meio oficial e quando estritamente necessário à concretização das atribuições;
- c) manter a absoluta cautela quando da exibição de dados pessoais em tela, por meio de impressões, ou, ainda, na gravação em meios eletrônicos, com escopo de inibir o acesso de terceiros não autorizados;
- d) não me ausentar do terminal sem encerrar a sessão de uso das bases, inibindo a prática de ações virtuais por terceiros não autorizados;
- e) não armazenar documentos de natureza particular em pastas institucionais;
- f) manter o sigilo dos dados pessoais ou informações sigilosas obtidas por força de minhas atribuições, mediante abstenção de compartilhamento e/ou divulgação a terceiros, sob pena de incorrer em sanções administrativas, civis e/ou penais decorrentes de eventual violação; e
- g) comunicar imediatamente ao Encarregado pelo tratamento de dados pessoais a ocorrência de qualquer ação ou omissão que contrarie o disposto neste termo, pelos meios formais disponibilizados pela instituição.

Rio de Janeiro, XX de XXXXXX de 20XX.



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:09, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112344402** e o código CRC **C5447F6A**.



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 TERMO DE REFERÊNCIA

MODELO DE ORDEM DE SERVIÇO / FORNECIMENTO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

1 - IDENTIFICAÇÃO DA ORDEM DE SERVIÇO / FORNECIMENTO			
Nº da OS/OF:	Data de Emissão:	Nº do Contrato:	Data do Contrato: Extrato DOERJ:



2 - IDENTIFICAÇÃO DA EMPRESA CONTRATADA			
Nome da Empresa:			
CNPJ:		Inscrição Estadual:	
Endereço:			
Cidade:		UF:	
CEP:	Telefone:	E-mail:	
Preposto:		Celular: E-mail:	

3 - ESPECIFICAÇÃO DOS PRODUTOS/SERVIÇOS E VOLUMES ESTIMADOS							
Item / Lote	ID SIGA	Descrição do Produto ou Serviço	Métrica	Valor Unitário (R\$)	Quantidade / Volume	Valor Total do item (R\$)	Parcela R\$ (esta coluna pode ser descartada em caso de pgto a vista)

Valor Total (R\$)	
--------------------------	--

4 – INSTRUÇÕES COMPLEMENTARES

5 – CIÊNCIA	
CONTRATANTE	
Gestor do Contrato	Fiscal Requisitante do Contrato
_____ nome ID nº	_____ nome ID nº
CONTRATADA	
PREPOSTO	
_____ nome CPF:	

-
- 
 Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).
-
- 
 Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:10, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112344269** e o código CRC **7A9F2576**.

Referência: Processo nº SEI-430002/000169/2025

SEI nº 112344269

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 V DO TERMO DE REFERÊNCIA

MODELO DE PLANILHA DE COMPOSIÇÃO DE PREÇOS

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

Processo SEI N° _____						
Ata de Registro de Preços N° ____/____						
Fornecedor:						
OBJETO:						
Lote 1						
Registro de Preços para contratação de empresa especializada no fornecimento de uma solução Web Application and API Protection – WAAP, contemplando a aquisição perpétua de hardware e software, com garantia de 36 (trinta e seis) meses, bem como a prestação de serviço de subscrição de software por 12 (doze) meses, com instalação/configuração, suporte técnico e treinamento da solução.						
Lote 2						
Registro de Preços para contratação de empresa especializada no fornecimento de solução Application Delivery Controller – ADC, contemplando aquisição perpétua de hardware e software, com garantia de 36 meses, com instalação/configuração, suporte técnico e treinamento da solução (LOTE II), conforme especificações e quantidades estabelecidas neste Termo de Referência e nos requisitos da contratação descritos no Estudo Técnico Preliminar.						
LOTE 1 - WAAP						
Item	ID SIGA	Descrição	Unidade de Fornecimento	Quantidade estimada	Valor Unitário (R\$)	Valor Total (R\$)
1	191788	Appliance de Web Application and API Protection (WAAP) - Hardware Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade			

2	191799	Appliance de Web Application and API Protection (WAAP) - Virtual Appliance, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade			
3	186917	Treinamento operacional para appliances WAAP	Unidade			
4	186914	Subscrição de solução para proteção em nuvem (SaaS), incluindo instalação, configuração e suporte técnico por 12 meses.	Turma			
5	187045	Franquia adicional de tráfego limpo para o Item 4	Anuidade			
6	186921	Treinamento operacional para WAAP SaaS	Terabyte			
Valor total do Lote 1						
LOTE 2 - ADC						
Item	ID SIGA	Descrição	Unidade de Fornecimento	Quantidade estimada	Valor Unitário (R\$)	Valor Total (R\$)
1	191789	Appliance de Controle de Entrega de Aplicação (ADC) e Balanceamento Dinâmico de Carga, com instalação, configuração, suporte técnico e garantia pelo período de 36 (trinta e seis) meses.	Unidade			
2	188007	Treinamento operacional para ADC	Turma			
Valor total do Lote 2						

- Os preços deverão contemplar discriminadamente todos os custos de cada item de acordo com as condições estabelecidas no Termo de Referência.



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:11, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112344339** e o código CRC **E85F8B6D**.

Referência: Processo nº SEI-430002/000169/2025

SEI nº 112344339

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 VI DO TERMO DE REFERÊNCIA

MODELO DE TERMO DE RECEBIMENTO PROVISÓRIO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

Identificação Contrato:	Nº da OS
Objeto:	
CONTRATANTE:	
Contratada:	

Por este instrumento, atestamos que os serviços integrantes da O.S. acima identificada, ou conforme definido no Modelo de Execução do contrato supracitado, foram recebidos nesta data e serão objetos de avaliação quanto à adequação da Solução de Tecnologia da Informação e à conformidade de qualidade, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato pela CONTRATANTE.

Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até ___ dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Termo de Referência do Contrato acima identificado.

De Acordo

CONTRATANTE	CONTRATADA
Membro da comissão fiscalizadora	Preposto

Nome:	Nome:
Matrícula:	Qualificação:

_____, _____ de _____ de 20__.



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:11, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112344547** e o código CRC **D7D88B9A**.



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 VII DO TERMO DE REFERÊNCIA
MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

Este anexo deve ser interpretado conforme as disposições do Termo de Referência do qual é parte integrante e indissociável.

1 – IDENTIFICAÇÃO			
CONTRATO Nº			Vigência:
CONTRATADA		CNPJ	
Nº DA OS/OFB			

2 – ESPECIFICAÇÃO DOS PRODUTOS/BENS E VOLUMES DE EXECUÇÃO						
SOLUÇÃO DE TIC						
Objeto:						
ID SIGA	Descrição do Produto ou Serviço	Métrica	Valor Unitário (R\$)	Quantidade / Volume	Valor Total (R\$)	Parcela 21/36 (R\$)
TOTAL						

3 – ATESTE DE RECEBIMENTO

Por este instrumento atestamos, que os serviços correspondentes à (link do documento) acima identificada foram prestados pela **CONTRATADA** e atendem às condições contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Termo de Referência do Contrato acima indicado.

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

5 – AUTORIZAÇÃO PARA FATURAMENTO

GESTOR DO CONTRATO

AUTORIZA-SE a **CONTRATADA** a apresentar as notas fiscais dos bens entregues relativos à supracitada (link do documento), no valor discriminado no item 2, acima.

Gestor do Contrato
Matrícula:

6 – CIÊNCIA

FISCAL TÉCNICO

Fiscal
Matrícula:

FISCAL REQUISITANTE

Fiscal
Matrícula:

PREPOSTO

Nome do Preposto da Contratada

CPF:

Nome da Contratada

Rio de Janeiro, ____ de _____ de _____



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:12, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112345156** e o código CRC **47BE228A**.

Referência: Processo nº SEI-430002/000169/2025

SEI nº 112345156

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 VIII DO TERMO DE REFERÊNCIA

MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

ESTE ANEXO DEVE SER INTERPRETADO CONFORME AS DISPOSIÇÕES DO TERMO DE REFERÊNCIA DO QUAL É PARTE INTEGRANTE E INDISSOCIÁVEL

DECLARAÇÃO DE NÃO UTILIZAÇÃO DE PRODUTOS PERIGOSOS E ADERÊNCIA AOS REQUISITOS DE SUSTENTABILIDADE AMBIENTAL

Atestamos, para fins de comprovação junto à COMISSÃO DE LICITAÇÃO – [ÓRGÃO] relativamente ao Edital nº_/2024 a empresa [NOME DA EMPRESA], CNPJ_, não emprega substâncias perigosas em seus produtos e prestação de serviços, de acordo com as exigências do Edital.

[CIDADE],__de_____de_____.



Documento assinado eletronicamente por **Charles Monteiro Guimarães, Diretor**, em 08/09/2025, às 15:47, 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 08/09/2025, às 15:54, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do [Decreto nº 48.209, de 19 de setembro de 2022](#) e no art. 4º do [Decreto nº 48.013, de 04 de abril de 2022](#).



Documento assinado eletronicamente por **Rosana Alves de Andrade, Analista de Sistemas**, em 08/09/2025, às 16:13, 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 **Fabio Ivo, Diretor**, em 08/09/2025, às 17:02, 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 **112344648** e o código CRC **BFBA96C4**.

Referência: Processo nº SEI-430002/000169/2025

SEI nº 112344648

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