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

ESTUDO TÉCNICO PRELIMINAR

SOLUÇÃO DE INTELIGÊNCIA DE AMEAÇAS (THREAT INTELL)

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

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

1.2. A solução de inteligência de ameaças (Threat Intell) tem por escopo o monitoramento e coleta de forma automatizada de potenciais ameaças na internet aos domínios hospedados no PRODERJ, promovendo, de forma antecipada, medidas defensivas e preventivas, gerando alertas cibernéticos em tempo real, com emissão de relatórios contendo análise de inteligência de ameaças.

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

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

1.5. O PRODERJ, instituição vinculada à Secretaria de Estado de Transformação Digital, atua como órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro. É responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, as bases de dados de vários órgãos estaduais e os diversos equipamentos hospedados no Datacenter do Estado. Diante o exposto, se torna essencial a garantia dos três pilares da segurança da informação, preconizada na ISO/IEC 27.000, quais sejam, confidencialidade, integridade e disponibilidade das informações. O declínio de apenas um desses pilares, mesmo que momentâneo, em decorrência de tentativas de sequestro de dados ou ataques cibernéticos de qualquer escala, resultam em danos incomensuráveis aos usuários dos serviços prestados através de qualquer sistema. O principal prejudicado é o cidadão, que tem atendidas suas necessidades básicas através de tais serviços.

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

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

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

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

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

1.11. O processo de transformação digital, atualmente em curso no Governo do Estado, aumenta ainda mais a demanda pela visibilidade de potenciais ameaças e incidentes de segurança, de modo que tenhamos a chance de mitigá-los, ou mesmo preveni-los.

1.12. Tem-se observado nos últimos tempos, um crescimento no número de tentativas de violação de dados aos ambientes tecnológicos, inclusive deste PRODERJ e de todo o Estado, colocando em sérios riscos o sigilo, a integridade e disponibilidade das informações.

1.13. Para evitar estes tipos de invasões e sequestro de dados e informações de extrema relevância, o PRODERJ se vê obrigado a proteger-se contra os ataques cibernéticos avançados direcionados, buscando mecanismos de detecção e análise que atuem de forma peremptória, automatizada e segura.

1.14. Considerando que o PRODERJ hospeda diversos sistemas e ativos de outros órgãos em sua infraestrutura, buscamos a melhoria contínua dos níveis de segurança na prestação do referido serviço de hospedagem prestado pela Autarquia. Desta forma, entendemos que a contratação de uma ferramenta de inteligência de ameaças que, através do monitoramento contínuo em diversos ambientes na internet, seja capaz de prever ataques aos sistemas e ativos hospedados no PRODERJ.

1.15. Da mesma maneira que os ataques cibernéticos estão em constante evolução, as camadas de proteção e detecção precisam evoluir para garantir a segurança do ambiente.

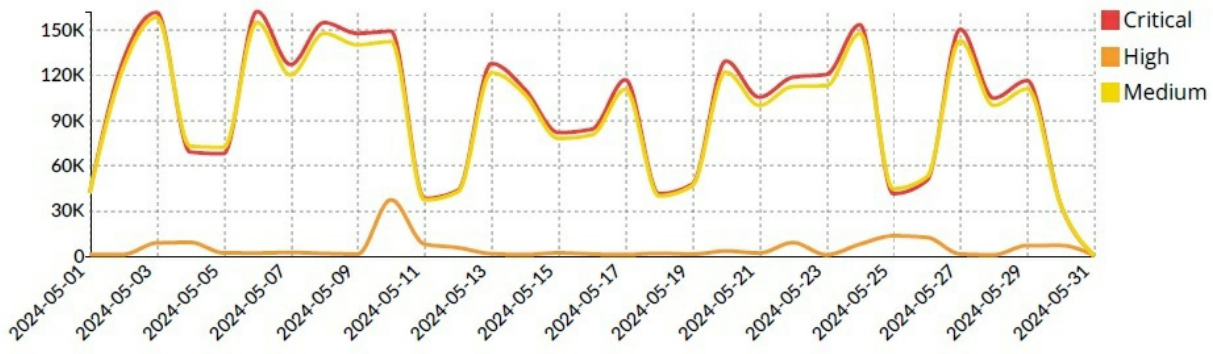
1.16. A tarefa de manter a área de TIC sempre alinhada às estratégias do PRODERJ constitui-se desafio permanente. Busca-se garantir em todas as questões relacionadas à infraestrutura de TI, que o foco se mantenha na estratégia e nas necessidades finalísticas da Autarquia. Além desta, existe também a tarefa e obrigação de manter o ambiente tecnológico em alta disponibilidade e de preservar a qualidade dos serviços por ele providos sempre alinhados às estratégias do PRODERJ.

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

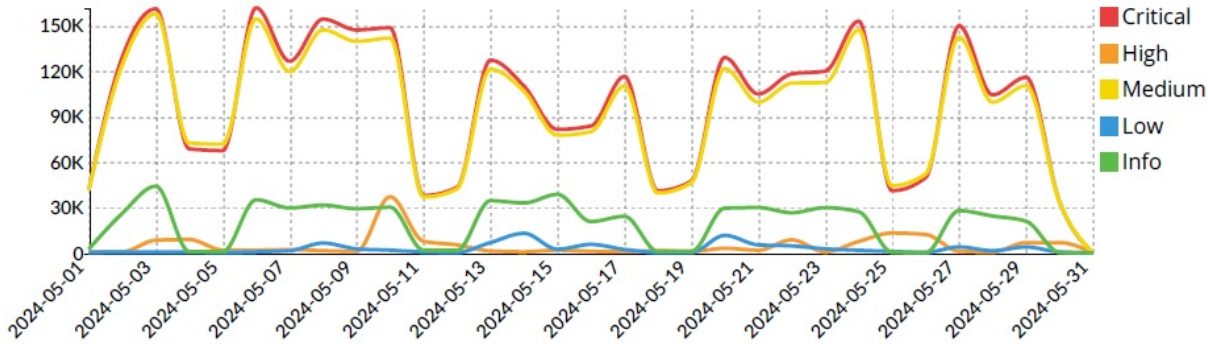
Ameaças por severidade

Critical	3,019,850
Medium	2,909,260
Info	603,601
High	146,655
Low	83,820

Timeline de intrusões (Criticas, Altas e Medias)



Timeline de intrusões (todas)



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

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

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

2. RESULTADOS PRETENDIDOS

A presente demanda visa a mitigação de diversas ameaças de segurança cibernética que afetam a rede governo, bem como obter os seguintes benefícios:

a) A oferta do presente Objeto visa robustecer e ampliar os quesitos de segurança para o domínio "*.rj.gov.br" contra ameaças cibernéticas, aprimorando a atual gestão de incidentes de segurança da informação;

b) Obter visibilidade sobre ameaças cibernéticas que estejam fora do alcance das ferramentas de segurança de perímetro, com o objetivo de prever ataques a ativos tecnológicos críticos;

c) Coibir a comercialização ilegal de credenciais de acesso que venham a ser exfiltradas no âmbito de algum órgão do Governo do Estado;

d) Detectar sites fraudulentos que venham a utilizar ilegalmente: marcas, nomes, logotipos e demais propriedades intelectuais pertencentes ao Governo do Estado;

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

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

3. CONTRATAÇÕES CORRELATAS

Não existe registro de objeto contratado que tenha pertinência por correlação ou por interdependência com o objeto deste estudo técnico.

4. INSTRUMENTOS DE PLANEJAMENTO

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

a) ID PCA no PNCP: 42498600000171-0-000053/2024;

b) Data de publicação no PNCP: 02/01/2024;

c) ID dos itens no PCA do PRODERJ (PNCP): vide tabela no subtópico 7.4. deste documento.

4.2. Previsão no PEDTIC (69709891, p 34 e 35) do PRODERJ:

a) **Objetivo Estratégico 1 - Prover, manter e atualizar a infraestrutura e as Soluções e Serviços de Tecnologia da Informação e Comunicação**: Prover continuamente a inovação tecnológica para compor e atualizar a infraestrutura, as Soluções e os Serviços de Tecnologia da Informação e Comunicação, atendendo às crescentes demandas da Autarquia e dos Órgãos do Poder Executivo Estadual, visando o desenvolvimento, manutenção, integração e a padronização da TIC do estado (Alinhamento ao PPA 2024-2027 - Programa: 0493 / Ações: 1293 e 1294);

b) **Objetivo Estratégico 2 - Ampliar a capacitação técnica e profissional dos servidores em TIC**: Promover a qualificação exponencial dos servidores por meio da capacitação e participação em eventos que desenvolvam e aprimorem suas competências e a gestão do conhecimento em TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1293);

c) **Objetivo Estratégico 3 - Aprimorar os Processos de TIC**: Promover a melhoria contínua dos processos, métodos e técnicas gerando uma maior efetividade na gestão e no uso dos recursos que fornecem as soluções de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ação 1294);

d) **Objetivo Estratégico 6 - Garantir os padrões de qualidade dos serviços e soluções de TIC**: Assegurar que os serviços de TIC prestados pelo PRODERJ atendam seus requisitos mínimos, suprindo as expectativas dos órgãos da Administração Pública Direta e Indireta, de modo que contribuam para a agregação de seus valores institucionais e o cumprimento de seus objetivos estratégicos, potencializando sua capacidade de entrega, reforçando a aptidão em produzir, entregar novas soluções e aprimorar as existentes, assim como, o fornecimento de uma infraestrutura inovadora que garantam que os recursos tecnológicos investidos sejam capazes de preservar e promover a segurança, a privacidade, a disponibilidade e a continuidade dos serviços públicos, reduzindo os riscos inerentes aos serviços de TIC (Alinhamento ao PPA 2024-2027 - Programa 0493 / Ações 1293 e 1294).

5. DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO

5.1. **Requisitos de Negócio**

5.1.1. Serviço de monitoramento e relatoria de ameaças cibernéticas externas que tenham como alvo os ativos de informação do Contratante.

5.1.2. A solução deverá possuir mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas (Telegram, Snapchat, Whatsapp e Messenger (Facebook)), mídias sociais (Twitter, Facebook, Instagram e Linkedin) e arquivos de logs, com acesso para gerenciamento via plataforma WEB.

5.2. **Requisitos de Capacitação**

5.2.1. A capacitação compreende os serviços de treinamentos (item 3 do lote único).

5.2.2. 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.

5.2.3. Deverá ser entregue para a contratante a proposta com o conteúdo do treinamento.

5.2.4. 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.

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

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

5.2.7. **Objetivo**

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

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

5.2.8. **Métrica**

O treinamento será contratado por turma de até 8 alunos.

5.2.9. **Carga horária**

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

5.2.9.2. 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.

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

5.2.10. **Forma de realização**

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

5.2.11. **Materiais didáticos e acessórios**

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

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

5.2.12. **Conteúdo programático**

5.2.12.1. 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.

5.2.12.2. 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.

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

5.3. **Requisitos Legais**

a) **Lei Federal nº 14.133/2021**, que trata das normas gerais sobre licitações e contratos administrativos;

b) **Lei Complementar nº 123/2006**, que estabelece normas gerais relativas ao tratamento diferenciado e favorecido a ser dispensado às microempresas e empresas de pequeno porte atualizada;

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

d) **Decreto Estadual 43.629/2012**, que dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços e obras pela Administração Pública Estadual Direta e Indireta e dá outras providências;

e) **Decreto Estadual nº 48.322/2023**, que dispõe sobre o enquadramento dos bens de consumo, adquiridos para suprir as demandas das estruturas da administração pública estadual, nas categorias de qualidade comum e de luxo;

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

g) **Decreto Estadual nº 48.760/2023**, que implementa o Plano de Contratações Anual - PCA e institui o Sistema PCA RJ, no âmbito da administração pública estadual direta, autárquica e fundacional;

h) **Decreto Estadual nº 48.778/2023**, que regulamenta as licitações pelos critérios de julgamento por menor preço ou por maior desconto, no âmbito da administração pública estadual direta, autárquica e fundacional;

i) **Decreto Estadual 48.816/2023**, que regulamenta a fase preparatória das contratações, de que trata a Lei nº 14.133, de 1º de abril de 2021, no âmbito da administração pública estadual direta, autárquica e fundacional;

j) **Decreto Estadual nº 48.817/2023**, que regulamenta a gestão e a fiscalização das contratações no âmbito da administração pública estadual direta, autárquica e fundacional e dá outras providências;

k) **Decreto Estadual nº 48.843/2023**, que regulamenta o sistema de registro de preços - SRP, no âmbito da administração pública estadual direta, autárquica e fundacional e dá outras providências;

l) **Decreto Estadual nº 48.865/2023**, que regulamenta as licitações pelo critério de julgamento por técnica e preço, no âmbito da administração pública estadual direta, autárquica e fundacional;

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

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

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

5.4. **Requisitos de Manutenção**

5.4.1. Todas as rotinas para fins de manutenção com vistas a plena e adequada execução do serviço de inteligência de ameaças, ao longo da vigência contratual estará a cargo da CONTRATADA. A solução tecnológica utilizada na prestação do serviço deverá estar disponível para acesso do CONTRATANTE por ao menos 99,5% do referido período contratual.

5.4.2. A Contratada deve disponibilizar ao menos uma das seguintes opções para abertura de chamados: ambiente web, número de telefone ou e-mail. O canal definido para comunicação e abertura de chamados deve estar disponível ao menos no regime 8x5, em horário comercial.

5.4.3. Os chamados abertos deverão obedecer aos níveis de serviço estabelecidos na tabela do tópico 5.11.1.4. deste documento.

5.4.4. **Requisitos Temporais**

Resguardado o cronograma previsto no subtópico 12.5.2.1 deste documento, não há outros requisitos temporais a serem considerados.

5.5. **Proteção de Dados Pessoais**

5.5.1. As partes (CONTRATANTE e CONTRATADA), no âmbito do quaisquer atividades oriundas da execução deste Estudo Técnico, observarão o regime legal concernente à proteção de dados pessoais, especialmente as diretrizes veiculadas pela Lei nº 13.709 de 14 de agosto de 2018 (LGPD) na realização de qualquer operação que se amolde ao preceito de tratamento de dados pessoais durante a execução do objeto.

5.5.2. A CONTRATADA deverá assinar Termo de Confidencialidade e Sigilo na forma do modelo a ser apresentado como anexo do futuro Termo de Referência.

5.5.3. Para atender aos ditames da Lei n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), a justificativa da necessidade compatível com as finalidades institucionais, assim como a apresentação de um relatório de impacto à proteção de dados pessoais (art. 5º, XVII, da LGPD) que aborde como serão usadas as tecnologias, deverá ser apresentada:

a) no momento da manifestação de interesse de participação da Intenção de Registro de Preços (IRP) pelos órgãos participantes; e

b) no momento da contratação realizada pelos órgãos não participantes.

5.5.4. As partes (CONTRATANTE e CONTRATADA), no âmbito de quaisquer atividades oriundas da execução deste Estudo Técnico, observarão o regime legal concernente à proteção de dados pessoais na realização de qualquer operação que se amolde ao preceito de tratamento de dados pessoais durante a execução do objeto.

5.5.5. Considerando a natureza dos dados tratados, pertinentes ao objeto desta contratação, a CONTRATANTE e a CONTRATADA 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.

5.5.6. A CONTRATADA 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.

5.5.7. A CONTRATANTE e a CONTRATADA devem adotar as medidas cabíveis para auxiliar na investigação, mitigação e reparação de cada um dos incidentes de segurança, quando identificada a responsabilização exclusiva, de uma parte e/ou outra.

5.5.8. A CONTRATADA, na execução dos serviços de plataforma de serviços digitais, deve auxiliar a CONTRATANTE, na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto no artigo 38 da Lei Federal nº 13.709/2018, no âmbito da execução deste objeto.

5.5.9. 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 pelo tratamento de dados pessoais;

f) Garantir que os respectivos colaboradores ou prestadores de serviços que tenham acesso aos dados pessoais no contexto deste Estudo Técnico cumpram as diretrizes protetivas dos dados pessoais, vinculando-os a um Termo de Confidencialidade.

5.5.10. Em se tratando de dados pessoais sensíveis, ambas as partes contratantes, deverão observar as hipóteses legais legitimadoras, nos moldes do Art. 11 da Lei 13.709/18, in verbis:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

5.5.11. O compartilhamento de dados deve ser operacionalizado em formato que assegure a necessária segurança da base de dados, como criptografia, anonimização, pseudonimização ou técnicas similares que alcancem idêntico escopo.

5.5.12. As partes (CONTRATANTE e CONTRATADA) deverão condicionar a realização das operações de tratamento de dados pessoais à assinatura de Termo de Confidencialidade, cujas cláusulas explicitem as obrigações e responsabilidades pertinentes.

5.5.13. O CONTROLADOR e OPERADOR deverão manter o registro das operações de tratamento de dados pessoais que realizarem, assim como estabelecer regras de boas práticas, considerando a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

5.5.14. O CONTROLADOR e OPERADOR, 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; e

f) as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos.

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

5.5.16. A responsabilidade pelo cumprimento das diretrizes contempladas na Lei nº 13.709/18, 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.

5.5.17. A CONTRATADA poderá responder por quaisquer danos, perdas ou prejuízos causados a CONTRATANTE, ou a terceiros, decorrentes do descumprimento da Lei Federal nº13.709/2018, não excluindo ou reduzindo essa responsabilidade a fiscalização do CONTRATANTE em seu acompanhamento.

5.5.18. A CONTRATADA deve atender à Política de Segurança da Informação instituída pela Instrução Normativa PRODERJ PRE nº 02, de 28 de abril de 2022 ou a que venha a substituí-la, e demais normativos correlatos publicados pelo CONTRATANTE.

5.6. **Requisitos Socioambientais**

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

5.7. **Requisitos Tecnológicos: Descrição pormenorizada, considerando todo o ciclo de vida do objeto a ser contratado, de forma precisa, suficiente e clara, por meio de especificações técnicas ou de desempenho do objeto usuais de mercado, vedando-se aquelas que, por excessivas, irrelevantes ou desnecessárias, limitem a competição**

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

5.7.1. **De arquitetura tecnológica**

5.7.1.1. Os requisitos tecnológicos de arquitetura da solução, relacionados ao item 1 do lote único, encontram-se no subtópico 3.1. do Anexo I - Especificações Técnicas do Objeto.

5.7.1.2. O Catálogo de Serviços correspondentes à Operação Assistida (item 2), econtra-se no subtópico 5.7.2.10. deste documento.

5.7.1.3. Os requisitos relacionados ao serviço de treinamento (item 3), encontram-se no subtópico 5.2. (Requisitos de Capacitação) deste documento.

5.7.1.4. Durante a reunião de kick-off, prevista no subtópico 5.7.2. (de projeto e de implementação) 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 tecnológico/operadcional e o consequente perfeito funcionamento da solução. Tais procedimentos devem estar alinhados às especificações técnicas descritas neste documento e em seu Anexo I.

5.7.2. **De projeto e de implementação**

5.7.2.1. A CONTRATADA deve realizar, nas dependências do CONTRATANTEJ ou de maneira remota, antes do início da prestação do serviço, uma

reunião inicial de projeto (kick-off) para a definição do plano de trabalho de instalação e configuração da solução, bem como dos escopos iniciais de monitoramento e relatoria.

5.7.2.2. Após a reunião de kick-off, a CONTRATADA deverá produzir e entregar ao CONTRATANTE o Projeto Executivo elaborado com base no quanto acertado ao longo da reunião, contemplando o planejamento, escopo de ativos críticos para monitoramento, definição de alertas, relatórios e outros possíveis requisitos para o início da prestação do serviço.

5.7.2.3. A Contratada deverá submeter previamente, por escrito, ao CONTRATANTE, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações acordadas.

5.7.2.4. 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.

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

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

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

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

5.7.2.9. O encaminhamento formal da solução contratada, considerados cada um dos itens do lote único do objeto, ocorrerá sempre por meio de emissão da Ordem de Serviço.

5.7.2.10. **Da implementação dos serviços de Operação Assistida**

I - Para o item 2 do lote único a CONTRATADA deverá, na reunião kick off, propor um plano de trabalho, contendo o detalhamento do escopo, cronograma estimado das entregas com seus prazos, quantitativo e valors estimados dos serviços. O Plano de Trabalho definitivo deverá ser entregue em até 10 (dez) dias úteis, contados da realização do kick off. Caso necessário, mediante pedido fundamentado da CONTRATADA, esse prazo poderá ser estendido, para garantir a boa execução dos serviços.

II - A CONTRATANTE será responsável pela análise e aprovação do Plano de Trabalho. Em caso de não conformidade(S) ou de alterações propostas pela CONTRATANTE, a CONTRATADA terá até 05 (cinco) dias corridos da comunicação para revisá-lo e encaminhar nova proposta para validação.

III - Caso a CONTRATADA não concorde com as alterações propostas pelo CONTRATANTE, haverá negociação, na qual as partes apresentarão suas considerações, fundamentando-se nos aspectos de qualificação e quantificação dos produtos/artefatos, na justa remuneração dos serviços e no interesse público.

IV - Para a execução de uma demanda poderá ser registrada mais de uma OS, devendo cada uma representar um conjunto inter-relacionado de funcionalidades ou artefatos que contemplem e delimitem uma fase ou iteração.

V - Qualquer alteração nas definições descritas na OS deverá gerar uma nova OS de solicitação de mudança, que será anexada a OS original.

VI - Poderá haver reedições do Plano de Trabalho, desde que demandadas pela CONTRATANTE e que sejam derivadas de mudança de escopo. O processo de execução do serviço poderá ser alterado a qualquer momento, em comum acordo entre CONTRATANTE e CONTRATADA.

5.7.2.11. **Catálogo de Serviços para Operação Assistida**

I - O Catálogo de Serviços relacionando as atividades necessárias e previstas para entrega do objeto, a necessidade / justificativa e as métricas para quantificação dos volumes de serviços necessários para alcance dos objetivos, está apresentado na tabela abaixo.

II - As atividades do Catálogo de Serviços representam mera expectativa, sendo admitida a execução de outras atividades que venham a ser necessárias ao longo do cumprimento do objeto, limitadas ao total de UST contratadas.

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

IV - Para a mensuração da quantidade de UST necessária para execução dos serviços, as USTs para execução da tarefa serão multiplicadas pelo fator referente ao nível de complexidade:

a) Complexidade BAIXA => 1;

b) Complexidade MÉDIA => 2;

c) Complexidade ALTA => 3.

CATÁLOGO DE SERVIÇOS					
ITEM	**TAREFA**	**DESCRIÇÃO**	**ENTREGÁVEL**	**NÍVEL DE COMPLEXIDADE**	**UST's MÍNIMAS PARA EXECUÇÃO DA TAREFA**
1	Inclusão de coleta em banco de dados	Inclusão de nova coleta em banco de dados público ostensivo ou de acesso restrito.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10
2	Inclusão de coleta em incidentes	Inclusão de nova coleta para os incidentes de segurança buscado diretamente no escopo de coleta.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
3	Inclusão no menu	Inclusão de item no menu do Sistema.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10

4	Inclusão em coleta	Inclusão de novos sistemas (AS), blocos ou endereços IP na coleta de vulnerabilidades conhecidas ou de tipo de pontos de exploração em aplicações e redes.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10
5	Criação de dashboard	Elaboração de novo dashboard de análise no Sistema.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
6	Inserção de alertas	Inserção de novos parâmetros para alertas de incidentes detectados pela ferramenta e envio de mensagens.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
7	Geração de relatório	Elaboração de relatório de avaliação da capacidade ofensiva de determinada ameaça cibernética.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
8	Ampliação de espaço	Ampliação do espaço cibernético de interesse do Contratante.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
9	Criação de indicador de coleta	Criação de novo indicador no sistema que tenha como fonte de dados a própria solução.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
10	Inclusão de incidente	Inclusão de novo tipo de incidente de segurança buscado diretamente no escopo de coleta, o qual inclui o desenvolvimento de interface de análise do novo tipo de incidente.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
11	Inclusão de coleta de vulnerabilidade	Inclusão de coleta de nova vulnerabilidade conhecida ou de novo tipo de pontos de exploração em aplicações e redes.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
12	Criação de indicador de processamento	Criação de novo indicador no sistema, tendo como fonte um conjunto de dados não-estruturados não originados da presente solução.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
13	Desenvolvimento de integração	Desenvolvimento e implantação de conector para integração e interoperabilidade com dispositivos de segurança de perímetro (firewall, proxy, IDS, IPS, servidor de e-mail).	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
14	Integração específica	Integração com outras soluções em uso no Contratante.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
15	Solicitação de Takedown	Solicitação de remoção de uma fonte de conteúdo criminoso ou fraudulento, abrangendo: domínios, aplicações, perfis em mídias sociais, etc.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10
16	Notificação automática sobre incidente de desfiguração de sítio	Customização e disponibilização de serviço de identificação de páginas com conteúdo incompatível com o original, persistindo, em todos os casos: URL da ocorrência; timestamp da detecção da ocorrência; categoria do incidente; e código fonte da página assinalada	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10
17	Notificação automática sobre incidente de indisponibilidade de domínios	Customização e disponibilização de serviço de assinalação de sítios indisponíveis a partir da Internet e notificação quando do retorno à disponibilidade, persistindo, em todos os casos: URL da ocorrência; timestamp da detecção da ocorrência; e categoria do incidente.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10
18	Notificação automática sobre diretórios sensíveis	Assinalação de diretórios com conteúdo sensível ou áreas administrativas acessíveis livre e indiscriminadamente a terceiros, , persistindo, em todos os casos: URL da ocorrência; timestamp da detecção da ocorrência; e categoria do incidente.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10
19	Notificação automática sobre exposição de dados	Assinalação de dados expostos em arquivos disponíveis inadvertidamente em aplicações web voltadas para a internet, , persistindo, em todos os casos: URL da ocorrência; timestamp da detecção da ocorrência; categoria do incidente; e código fonte da página assinalada	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	BAIXA (x1)	10
20	Notificação automática de honeypot	Customização e disponibilização de serviço de notificação de ativo no escopo de interesse potencialmente envolvido em ataque a honeypot, identificando e armazenando, sempre que disponível, as seguintes informações: endereço IP e porta associada à origem potencialmente maliciosa; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP da origem potencialmente maliciosa; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; login e senha em caso de tentativa de autenticação no honeypot; e exemplares dos malwares obtidos.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10

21	Notificação automática de vulnerabilidade em infraestrutura	Customização e disponibilização de serviço de notificação de serviços dos protocolos RDP, FTP, VNC e Telnet cujo acesso possa ocorrer remotamente e permita ao atacante acesso à área administrativa do servidor-alvo em função de acesso sem a autenticação do usuário ou com autenticação anônima , apresentando: vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração; timestamp da detecção da ocorrência; endereço IP e porta associada à vulnerabilidade ou ponto de exploração; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP onde a URL da ocorrência está hospedada; identificação do provedor de conexão (ISP) do endereço IP; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste; as classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE); os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web; o cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS; a relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
22	Notificação automática de vulnerabilidade apta a causar indisponibilidade de serviços	Customização e disponibilização de serviço de notificação de servidores dos protocolos DNS e NTP suscetíveis a amplificação de ataques de negação de serviço (Denial of Service – DoS), transferência de zona ou configurados de forma a resolver domínios maliciosamente, conduzindo o usuário a páginas falsas, , apresentando: vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração; timestamp da detecção da ocorrência; endereço IP e porta associada à vulnerabilidade ou ponto de exploração; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP onde a URL da ocorrência está hospedada; identificação do provedor de conexão (ISP) do endereço IP; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste; as classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE); os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web; o cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS; a relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
23	Notificação automática de vulnerabilidade apta a ocasionar exposição de dados	Customização e disponibilização de serviço de notificação de bancos de dados ou storages PostgreSQL, MySQL, SQLServer, Oracle e Elastic Search, MongoDB, Iomega cujo acesso possa ocorrer remotamente sem a presença de autenticação ou que permitam ataque de força bruta para o acesso indevido , apresentando: vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração; timestamp da detecção da ocorrência; endereço IP e porta associada à vulnerabilidade ou ponto de exploração; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP onde a URL da ocorrência está hospedada; identificação do provedor de conexão (ISP) do endereço IP; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste; as classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE); os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web; o cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS; a relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
24	Notificação automática de vulnerabilidade na implementação de criptografia	Customização e disponibilização de serviço de notificação de sistemas suscetíveis, no mínimo, aos ataques HeartBleed, Freak, Poodle, BEAST e Logjam, apresentando: vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração; timestamp da detecção da ocorrência; endereço IP e porta associada à vulnerabilidade ou ponto de exploração; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP onde a URL da ocorrência está hospedada; identificação do provedor de conexão (ISP) do endereço IP; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste; as classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE); os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web; o cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS; a relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10

25	Notificação automática de vulnerabilidade no uso de protocolos legados	Customização e disponibilização de serviço de notificação de sistemas suscetíveis, no mínimo, aos ataques HeartBleed, Freak, Poodle, BEAST e Logjam, apresentando: vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração; timestamp da detecção da ocorrência; endereço IP e porta associada à vulnerabilidade ou ponto de exploração; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP onde a URL da ocorrência está hospedada; identificação do provedor de conexão (ISP) do endereço IP; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste; as classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE); os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web; o cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS; a relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
26	Notificação automática de vulnerabilidade em serviços	Customização e disponibilização de serviço de notificação de serviços FTP, NetBIOS, SMB, SSH e VPN cuja configuração equivocada possa permitir o mapeamento de ativos em redes não públicas e identificação de serviços acessíveis , apresentando: vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração; timestamp da detecção da ocorrência; endereço IP e porta associada à vulnerabilidade ou ponto de exploração; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP onde a URL da ocorrência está hospedada; identificação do provedor de conexão (ISP) do endereço IP; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste; as classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE); os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web; o cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS; a relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
27	Notificação de vulnerabilidade em IOT	Customização e disponibilização de serviço de notificação de equipamentos e artefatos classificados como Internet das Coisas (Internet of Things – IoT) acessíveis remotamente por meio da internet, dentre os quais, os dispositivos de rede, as impressores e as câmeras de monitoramento , apresentando: vulnerabilidade conhecida, a respectiva CVE, CWE e exploit disponível para exploração; timestamp da detecção da ocorrência; endereço IP e porta associada à vulnerabilidade ou ponto de exploração; domínio reverso associado ao endereço IP da ocorrência; geolocalização do endereço IP onde a URL da ocorrência está hospedada; identificação do provedor de conexão (ISP) do endereço IP; payload de resposta obtido por meio da requisição formulada como teste da vulnerabilidade notória ou ponto de exploração; resposta dos protocolos de criptografia aceitos pelo servidor objeto do teste; as classificações de vulnerabilidades associadas à ocorrência observada (Common Vulnerabilities and Exposures do MITRE); os componentes utilizados pela aplicação, como, por exemplo, tipo de CMS, no caso de vulnerabilidades envolvendo aplicações web; o cálculo da severidade da vulnerabilidade seguindo o padrão de mercado do NIST CVSS; a relação atualizada das principais Google Dorks utilizadas para identificação de vulnerabilidades no Escopo Interno.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
28	Notificação de incidente reportado em serviço de compartilhamento de desfigurações	Customização e disponibilização de serviço de notificação automática sobre incidente pertinente ao escopo detectado nos portais Zone-H, Defacer ID e Mirror-H, persistindo URL da ocorrência; finalidade do domínio no contexto coletado (distribuição, comando e controle, redirecionamento para atividade maliciosa ou outra classificação plausível); timestamp da detecção do incidente; detalhes sobre a autoria do incidente (no caso de desfiguração, o grupo ao qual se atribui o ataque, bem como seu indivíduo notificador); características da máquina atacada (sistema operacional, servidor web e a forma de ataque declarada); registros em espera de validação (onhold), no caso de incidentes de desfiguração, sendo que o processo de coleta deve incluir a validação automatizada das desfigurações, realizando uma Coleta no Escopo Direto, de modo a impedir a persistência de falsos positivos desse tipo de incidente; evidência do ocorrido, no caso de incidentes de desfigurações, consubstanciada na forma de printscreen e de obtenção do código HTML fonte da página afetada.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
29	Notificação de incidente reportado em plataforma de bug bounty	Customização e disponibilização de serviço de notificação automática sobre incidente pertinente ao escopo detectado nas plataformas Open Bug Bounty e Bug Heist, persistindo URL da ocorrência; finalidade do domínio no contexto coletado (distribuição, comando e controle, redirecionamento para atividade maliciosa ou outra classificação plausível); timestamp da detecção do incidente.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10

30	Notificação de incidente reportado em blacklist	Customização e disponibilização de serviço de notificação automática sobre incidente pertinente ao escopo em blacklist	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
31	Notificação de incidente reportado em serviço de notificação de phishing	Customização e disponibilização de serviço de notificação automática sobre incidente pertinente ao escopo detectado em plataformas de notificação de phishing (Phishtank e Openphish), persistindo URL da ocorrência; finalidade do domínio no contexto coletado (distribuição, comando e controle, redirecionamento para atividade maliciosa ou outra classificação plausível); timestamp da detecção do incidente; entidade alvo da atividade maliciosa, no caso de phishing (a página ou serviço de quem se pretendia simular); artefato malicioso identificado como provocador no caso do phishing;.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	MÉDIA (x2)	10
32	Notificação de incidente reportado em plataforma de compartilhamento de malware	Customização e disponibilização de serviço de notificação automática sobre incidente pertinente ao escopo detectado em plataformas de notificação de compartilhamento de malware (VirusTotal, HybridAnalysys e Any.run), persistindo URL da ocorrência; timestamp da detecção do incidente; evidência e indicação do domínio do Escopo Interno afetado, no caso de malwares.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
33	Notificação automática de ativo do escopo envolvido em download de conteúdo em redes p2p	Customização e disponibilização de serviço de notificação automática sobre atividade de ativo do escopo na rede BitTorrent, persistindo informações do endereço ip afetado (whois, reverso e titularidade) e do conteúdo acessado (com a respectiva categoria)	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
34	Notificação automática de menção ao escopo em fontes que apresentam os dados dispersos e de forma não-estruturada	Customização e disponibilização de serviço de notificação automática sobre publicações que versarem sobre a incitação, a ameaça ou o relato de ataque cibernético a ativos do Escopo Interno nas seguintes modalidades: negação de serviço (Denial of Service - DoS); desfiguração de página (defacement), pautado pela ontologia disposta em dicionário a ser fornecido pela CONTRATANTE; vazamento de dados, incluindo bases de dados (dumps), credenciais de acesso (leaks), exposições de dados pessoais (exposed); exposições de configurações sensíveis de aplicações ou de seus respectivos códigosfonte; exposições de dados sensíveis, de acordo com a ontologia pautada em palavras-chave provenientes de um dicionário a ser fornecido pela CONTRATANTE; invasão de sistema ou equipamento; phishing; ransomware; ferramentas e exploits. Os registros que preencham os temas acima descritos devem ser coletados, sempre que possível e obedecendo as características de cada serviço ou canal de comunicação, com a persistências dos seguintes dados: URL da ocorrência; timestamp da detecção da ocorrência; código fonte da postagem ou o conteúdo relevante assinalado, de modo que se a postagem original venha a ser removida pelo seu autor ou por terceiros, o conteúdo do registro seja ainda acessível; domínios e URL mencionadas (incluídas credenciais de acesso com base em endereços de correio eletrônico) que estiverem associadas ao escopo de incidência da coleta; mídias anexadas ao texto da postagem (imagens e vídeos) em qualquer um dos canais monitorados; dados disponíveis sobre o autor/canal da publicação, tais como a imagem/avatar, o texto descritivo do perfil ou canal, a localidade declarada do perfil ou canal, o número de seguidores ou amigos, o número de perfis que o autor segue e a quantidade total de publicações (aplicável às coletas de incidentes sobre redes sociais e canais de compartilhamento de vídeos e dos canais de comunicação); endereço IP indicado como alvo da ferramenta/exploit; domínio indicado como alvo da ferramenta/exploit; e classificação de CVE que foi atribuída à ferramenta/exploit.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
35	Coleta sobre atividades de APTs (Advanced Persistent Threats)	Integração automatizada da coleta sobre APTs com ferramentas de proteção de perímetro, abrangendo, no mínimo, Indicadores de Comprometimento (Ips, domínios, hashes, etc), informações sobre Táticas, Técnicas e Procedimentos (TTPs) e sobre ferramentas utilizadas	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
36	Desenvolvimento de interfaces de consultas em estruturas de pesquisa estáticas	Customização e disponibilização de interface de apresentação de cada cenário especificado de forma gráfica e transparente. Cada consulta, quando pertinente, deve disponibilizar o histórico de eventos relacionados, de modo a correlacionar as ocorrências sob a dimensão temporal. As informações devem ser apresentadas, no mínimo, segundo os seguintes cenários de interesse: Domínio; Categoria de Incidente; Atacante; Vulnerabilidade; País; APT; e Honeypots. Estes cenários devem agrupar os elementos pertinentes e apresentar links para outros, quando cabível. O Cenário de Domínio deve apresentar, no mínimo: Relação de incidentes detectados, agrupados por categoria e por evento; Relação de atacantes com alvo no domínio; Relação de eventos de indisponibilidade de sítio, contendo duração aproximada. O Cenário de Categoria de Incidente deve permitir a Categorização dos incidentes em Desfiguração de Sítio; Indisponibilidade de Domínio; Diretórios Sensíveis; Exposição de Dados; e Inclusão em Blacklist. Para cada categoria de incidente, quando houver a caracterização de um ataque, apresentar relação de: atacantes, classificados de acordo com os graus de atividade (frequência de ataques somados à frequência de posts em mídias sociais); domínios e subdomínios com maior quantidade de ataques, total e por categoria.	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10

37	Desenvolvimento de interfaces de consultas em estruturas de pesquisa dinâmica	A interface deve ser capaz de: realizar busca textual com base em filtro de texto completo (full-text search) sobre todos os tipos de registros e todos os campos de conteúdo e de características gerais. A busca em texto completo deve, ainda, permitir a indicação de campo de conteúdo específico, por exemplo: autor, domínio, título; realizar busca de registros com base em filtro de expressões regulares (regular expression ou regex) de modo a permitir a busca por padrão de texto sobre todos os tipos de registros e todos os campos de conteúdo e de características gerais; realizar busca com base em filtro na origem do dado (fontes onde as coletas foram realizadas); realizar busca com base em filtro no tipo do dado (por exemplo: vulnerabilidades identificadas, phishings, ransomware, etc); realizar busca com base em filtro nas datas dos incidentes, sendo possível a fixação de intervalos para pesquisa (intervalo mensurado entre horas e anos); realizar buscas de acordo com características gerais (por exemplo: endereço IP, domínio registado) ou específicas (por exemplo: o status do registro de phishing) das ocorrências; realizar buscas com base em lapso temporal; combinar múltiplos filtros sucessivos que devem contemplar todos os campos dos registros; realizar a contagem de termos de quaisquer dos tipos de registro contidos na base de dados de coletas (por exemplo: nome de atacante, domínio, ISP).	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10
38	Relatórios customizáveis	Emissão de relatórios customizáveis com base tanto nas Consultas em Estruturas de Pesquisa Estáticas quanto nas Dinâmicas, priorizando-se recursos gráficos que permitam maior velocidade na obtenção da consciência situacional; a elaboração de gráficos de diversos tipos que respondam dinamicamente à combinação de múltiplos filtros, simultâneos ou sucessivos, e que sejam exportados junto aos dados brutos selecionados; a elaboração de tabelas dinâmicas, que permitam a inclusão ou remoção de colunas na exportação dos dados ou geração de gráficos; a exportação dos dados de uma consulta, no mínimo, nos formatos CSV, XML e JSON; e a importação dos dados, no mínimo, nos formatos CSV, XML e JSON	Relatório citado no subtópico 12.9.1., inciso II e suas alíneas, do Estudo Técnico Preliminar	ALTA (x3)	10

5.7.2.12. **Considerações sobre o uso da medição em UST (Unidade de Serviço Técnico) para o item 2 (Operação Assistida)**

I - Visando atender às necessidades específicas da administração Pública, são previstos no presente documento "Serviço de Operação Assistida" item 2 cujas tarefas poderão ser contratados sob demanda para atender as características específicas. Tais serviços demandarão customizações e configurações. Deverão ser mensurados por Unidade de Serviço Técnico (UST), levando em consideração os níveis de complexidade das tarefas, o esforço empreendido e os resultados esperados, assegurando o correto uso de recursos financeiros.

II - A utilização da métrica por UST na medição do item 2 leva em consideração a própria lógica das tarefas componentes do seu escopo, caracterizadas por resultados medidos conforme especificações previamente estabelecidas em um **Catálogo de Serviços** detalhado.

III - Unidade de Serviço Técnico é uma métrica para a medição do esforço na execução de um serviço que envolva atividade humana não mensurável previamente com precisão, sendo certo que qualquer técnica com precisão de mensuração que seja inferior a 90%, é candidata a ser substituída pela UST. É bastante utilizada em contratos de prestação de serviços que envolvam diversos tipos de serviços com variados graus de especificidade.

IV - Saliente-se que tal opção, neste certame, está em conformidade com as orientações do Egrégio Tribunal do Contas da União sobre o tema constantes no Acórdão nº 2037/2019-TCU. Plenário. TC014.760/2018-5.

5.7.3. **Das atualizações do sistema**

A CONTRATADA deverá realizar a atualização da solução fornecida sempre que sejam disponibilizadas atualizações pelo fabricante.

5.7.4. **Do suporte técnico**

5.7.4.1. Durante todo o período da subscrição a Contratada será responsável pelo suporte técnico da ferramenta tecnológica que compõe a solução Threat Intel (Item 1 do Lote Único);

5.7.4.2. Em caso de interrupção ou indisponibilidade da solução, a Contratada se compromete a realizar as correções necessárias à reativação da mesma, e a prevenção de novas interrupções, respeitando os prazos de atendimento.

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

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

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

5.7.4.6. Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado no sistema, observados os níveis de severidade, na forma da tabela que consta no subtópico 5.11.1.4. deste documento.

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

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

5.7.4.9. 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.

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

5.7.4.11. 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.

5.7.4.12. 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.

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

5.7.4.14. 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.

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

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

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

5.7.5.3. Serão aceitos certificados ou diplomas originais, que comprovem as formações e /ou experiências exigidas.

5.7.6. **De metodologia de trabalho**

5.7.6.1. 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.

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

5.7.6.3. 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;

5.7.6.4. 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.

5.8. **Requisitos Materiais e Humanos**

5.8.1. Materiais, insumos e acessórios necessários ao perfeito funcionamento itens previstos no lote único deverão ser arcados pela CONTRATADA, sem custos adicionais para a CONTRATANTE.

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

5.8.3. 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 de solução tecnológica (software) em modalidade subscrição, e respectivos serviços de operação assistida e 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.

5.8.4. **Quantitativo de usuários:**

Não se aplica

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

5.8.5.1. Considerada a prestação do Suporte Técnico, o horário de funcionamento do órgão é entre 09hs e 18hs, de segunda a sexta-feira, resguardadas eventuais emergências cuja ocorrência se dê em qualquer horário e dia.

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

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

Na forma do subtópico 5.5.18. deste documento, no que couber.

5.8.7. **Disposições normativas internas:**

Na forma do subtópico 5.5.18. deste documento.

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

Na forma do subtópico 5.7.1.4 deste documento.

5.9. **Providências a serem adotadas pela administração previamente à celebração do contrato**

Não há providências a serem adotadas que sejam antecedentes e necessárias à celebração do contrato.

5.10. **Fiscalização e Acompanhamento do Contrato**

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

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

5.11. **Acordo de Nível de Serviço**

5.11.1. **Para os serviços de subscrição**

5.11.1.1. **Finalidade:** Garantir a qualidade dos Serviços de subscrição.

5.11.1.2. **Periodicidade:** Trimestral

5.11.1.3. **Início da medição:** Após a emissão do Termo de Recebimento Definitivo com anotação no Registro de Ocorrências.

5.11.1.4. **Mecanismo de cálculo:** Na forma da tabela abaixo:

Severidade	Descrição	Tempo do 1º contato após abertura do chamado de Suporte Técnico	Tempo de solução após o 1º contato
Alta	Solução totalmente inoperante	até 2 horas	até 3 horas
Média Alta	Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução	até 6 horas	até 6 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 24 horas	até 12 horas
Baixa	Solicitações de informações diversas ou dúvidas sobre a solução	até 48 horas	até 24 horas

5.11.2. **Para os serviços de operação assistida**

5.11.2.1. **Finalidade:** Garantir a qualidade dos Serviços de Operação Assistida.

5.11.2.2. **Periodicidade:** eventual, ao final das tarefas demandadas na Ordem de Serviço, para fins de ateste de Nota Fiscal e emissão do Termo de Recebimento Definitivo.

5.11.2.3. **Início da medição:** Após a emissão do Termo de Recebimento Definitivo com anotação no Registro de Ocorrências.

5.11.2.4. **Mecanismo de cálculo:** Na forma da tabela abaixo:

Severidade	Descrição	Tempo de atraso do prazo de execução previsto na Ordem de Serviço	Tempo de atraso do prazo repactuado mediante requerimento justificado da CONTRATADA
Alta	Solução totalmente inoperante em razão do atraso injustificado na entrega das tarefas	até 2 dias	até 2 dias
Média	Solução parcialmente inoperante em razão do atraso injustificado na entrega das tarefas	até 2 dias	até 2 horas
Baixa	Solução totalmente operante, mas com atraso injustificado na entrega das tarefas	até 2 dias	até 2 dias

5.11.3. **Para os serviços de treinamento (item 3 do lote)**

5.11.3.1. **Finalidade:** Garantir a qualidade dos Serviços de Treinamentos.

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

5.11.3.3. **Início da medição:** Após a emissão do Termo de Recebimento Definitivo com anotação no Registro de Ocorrências.

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

I - I (insatisfatório) – 0 a 25%;

II - R (regular) – 26 a 50%;

III - B (bom) – 51 a 75%;

IV - MB (muito bom) – 76 a 100%.

5.12. **Sanções**

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

I - **Para os serviços de subscrição (item 1 do lote único):**

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

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

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

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

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

II - **Para os serviços de operação assistida (item 2 do lote único):**

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

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

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

d) 0,20% no valor do item correspondente do mês de referência, por dia de atraso injustificado, após o vencimento dos prazos previstos na Ordem de Serviço da demanda categorizada como "alta", até o limite de 5 dias.

e) 0,40% no valor do item correspondente do mês de referência, por dia de atraso injustificado, após o vencimento dos prazos repactuados para conclusão da demanda categorizada como "alta", até o limite de 5 dias.

III - **Para o serviço de treinamento (item 3 do lote único):**

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).

5.12.3. 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.

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

5.12.5. As multas por não cumprimento dos níveis de serviço serão descontadas da garantia de contrato prevista no subtópico 12.13 deste documento, resguardado o limite da mesma.

5.12.6. 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.

5.12.7. 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.

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

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

5.12.10. 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.

5.12.11. 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.

6. NATUREZA DO OBJETO DA CONTRATAÇÃO

6.1. Os itens que integram o objeto previsto 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 SERVIÇOS COMUNS ou usuais de mercado.

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

a) O item 1 é medido em unidades e correspondem a serviço de subscrição (licença temporária) de software, com natureza contínua;

b) O item 2 é medido por Unidade de Serviço Técnico (UST) e corresponde a serviço sob demanda, com natureza contínua;

c) O item 3 é medido por turmas (de até 8 alunos) e corresponde a serviço de treinameno sob demanda, de natureza contínua.

7. ESTIMATIVAS DAS QUANTIDADES A SEREM CONTRATADAS

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

7.2. A quantidade estimada de subscrição (item 1) é de 1 unidade por órgão contratante.

7.3. A quantidade estimada de UST para o serviço de operação assistida (item 2) considerou a ocorrência mínima de 1 evento para cada uma das atividades previstas no catálogo de serviços ao longo de cada um dos 12 meses de contratação, sendo certo que a natureza do serviços em tela é de atividade "sob demanda". Nesse passo, serão 800 UST multiplicadas por 12 (meses de contrato) = 9.600 UST a serem utilizadas sob demanda.

7.4. A quantidade estimada para o treinamentos (item 3) considerou a capacitação de duas turmas de servidores, totalizando um potencial de treinamento de até 16 (dezesseis) técnicos, a critério do PRODERJ. Tais quantitativos consideram o grau de relevância, na infraestrutura, das soluções tecnológicas a serem contratadas às quais os treinamentos estão relacionados. Considera ainda eventuais desligamentos de servidores treinados, de forma a viabilizar o treinamento de um outro servidor. Saliente-se que a definição de unidade por turma é a usual de mercado, verificada recorrentemente nas licitações públicas.

LOTE ÚNICO					
Item	**ID SIGA/RJ**	**ID PCA (PNCP)**	**Descrição**	**Métrica**	**Quantidade**
1	189023	em catalogação	Subscrição de Solução Threat Intel com suporte técnico, pelo período de 12 meses	Unidade	1
2	189024	em catalogação	Serviço de Operação Assistida para Solução de Threat Intel	UST	9.600
3	189028	em catalogação	Treinamento operacional na Solução Threat Intel	Turma	2

8. LEVANTAMENTO DE MERCADO

8.1. **Levantamento das Soluções**

Solução 1 - Utilização de ferramentas OSINT Gratuitas

Para o atendimento desta demanda, existe a possibilidade do emprego de diversas ferramentas open source gratuitas, para o monitoramento dos domínios e/ou ativos tecnológicos que farão parte do escopo. Neste cenário, o PRODERJ opera e mantém um conjunto de ferramentas open source a fim de realizar a monitoria e relatoria sobre os domínios/subdomínios a serem protegidos.

- **Vantagens:** Por conta das ferramentas gratuitas e disponíveis na internet, esta opção não envolve custos diretos com a contratação de serviço ou solução tecnológica.

- **Desvantagens**: São necessárias diversas ferramentas open source para desempenhar as funcionalidades de uma solução corporativa/enterprise. Ainda assim, tal operação seria algo complexo e desconexo, e os relatórios de inteligência, justamente por estarem difusos entre várias soluções, não possuiriam a mesma assertividade daqueles oriundos de uma ferramenta capaz de centralizar o resultado do monitoramento de diversas fontes de dados. Haveria ainda a obrigação do PRODERJ em operar tais soluções gratuitas, correlacionado os dados de inteligência produzidos, de maneira a manter a infraestrutura de tal solução, o que implicaria em designar quadros técnicos especializados para a operação e manutenção da solução.

Solução 2 - Contratação de Serviço Gerenciado de Inteligência de Ameaças

Neste cenário, seria disponibilizada a contratação de uma empresa especializada na prestação do serviço de monitoramento e relatoria para inteligência de ameaças, onde o Contratante teria acesso apenas aos relatórios de inteligência, sem qualquer tipo de gerenciamento direto na ferramenta utilizada pela Contratada, que seria responsável pela execução de quaisquer alterações no escopo de monitoramento/relatoria.

- **Vantagens:** O Contratante receberia da Contratada apenas os relatórios e alertas produzidos pela ferramenta, sem a necessidade de alocar quadros técnicos para a operação da solução.

- **Desvantagens:** Neste cenário, a Contratada faria uma composição de produtos para o atendimento ao objeto, pois seriam somados os custos de licenciamento mais a mão-de-obra operacional, para que os entregáveis possam ser gerados e enviados ao Contratante na forma de relatórios. Em outras palavras: este cenário/opção permitiria apenas a contratação do “pacote completo”, o que poderia onerar demasiadamente a contratação.

Ainda neste cenário, o Contratante se torna dependente de tempos de resposta da Contratada, o que pode atrasar alguma tomada de decisão ou algum tipo de ação do Contratante.

Solução 3 - Contratação de Ferramenta Threat Intel via Subscrição (SaaS)

Neste cenário, a Contratada fornece o direito de uso da ferramenta ao Contratante por um período definido. Neste caso, devem ser disponibilizados, em caráter opcional: serviço de operação assistida (com catálogo de serviços relacionados) e treinamento na solução, oferecidos para que o Contratante tenha plenas condições de utilização da ferramenta durante a vigência contratual.

- **Vantagens:** A modularidade dos itens pode ser mais compatível com o formato "Ata de Registro de Preços", já que possibilita uma adesão mais customizada ao objeto. Neste cenário, o Contratante pode aderir somente ao item de subscrição do software, caso tenha condições de operar a solução, ou ainda, aderir ao item de operação assistida, que oferece um catálogo com todos os serviços relacionados à operação cotidiana da ferramenta. Esta opção permite que o Contratante tire o máximo de proveito da solução tecnológica, independentemente do seu nível de maturidade em Segurança da Informação.

- **Desvantagens:** Caso o Contratante opte por não aderir ao item de "serviço de operação assistida", ele deverá operar todos os aspectos da solução, o que pode ser um problema, especialmente para aqueles Contratantes que não possuem mão-de-obra especializada em Segurança da Informação.

Solução 4 - Aquisição de Ferramenta Threat Intel

Neste cenário, o fornecimento da solução seria através da aquisição do conjunto hardware + licença perpétua do software, com garantia de suporte e atualização por um período definido.

- **Vantagens:** Na modalidade "aquisição perpétua", O PRODERJ manteria, após o término da garantia, algumas das funcionalidades de monitoramento e relatoria previamente configuradas na ferramenta. A aquisição proporcionaria também uma redução da curva de aprendizado que ocorre a cada troca de tecnologia.

- **Desvantagens:** Os fabricantes líderes do mercado, via de regra, oferecem este tipo de solução na forma de subscrição ou serviço gerenciado. Tal prática é usualmente adotada pelo mercado, pois é da natureza das soluções de threat Intel, a necessidade constante em se buscar proativamente novas fontes de informações nos confins da internet, incluindo fóruns obscuros, mídias sociais, grupos em apps de mensageria instantânea e etc. Em outras palavras, Threat Intel é o tipo de solução que precisa ser constantemente alimentada com novas informações, o que envolve uma busca proativa e não-automatizada por tais fontes, tarefa normalmente realizada pela contratada, durante a vigência contratual. O formato "aquisição perpétua" pressupõe que, após o término do contrato, o órgão contratante deverá estar pronto para assumir a tarefa dele mesmo proceder com esta busca proativa, a fim de configurar a solução adquirida, para que a mesma passe a monitorar novas fontes de informação. O contratante deverá também, além de manter as fontes de dados atualizadas, analisar todos os alertas que serão gerados pela ferramenta, para finalmente adotar medidas para mitigação de possíveis vulnerabilidades. Por fim, tal modalidade de contratação, se aplicada a este objeto, traria ainda a desvantagem de uma desnecessária dependência tecnológica com o fornecedor da solução.

8.2. Avaliação Comparativa (Benchmarking)

A seguir, podemos ver a tabela comparativa entre alguns players de mercado para solução Threat Intel. Na tabela, são elencadas algumas características técnicas relevantes para a referida solução.

Comparativo features - Threat Intell - 2024					
Características	**FABRICANTE / SOLUÇÃO**				
	HARPYA	**CROWDSTRIKE**	**PALO ALTO**	**KASPERSKY**	**IBM**
Agregar dados de fontes públicas	SIM	SIM	SIM	SIM	SIM
Agregar dados de fontes privadas	SIM	**NÃO**	SIM	SIM	SIM
Feeds de inteligência de ameaças de terceiros	SIM	SIM	SIM	SIM	**NÃO**
Suporte a integração com ferramentas de alerta e SIEM	SIM	**NÃO**	SIM	SIM	SIM
Informações em tempo real	SIM	SIM	SIM	SIM	**NÃO**
Monitoramento de Botnets	SIM	**NÃO**	SIM	SIM	**NÃO**
Emissão de Relatórios	SIM	SIM	SIM	SIM	SIM

8.3. Análise de Projetos Similares

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

	ÓRGÃO / ENTIDADE	**Nº Contrato / Edital**	**Valor (R$)**	**Fornecedor**	**Natureza do Objeto**	**Período de subscrição / garantia do produto**	**ANÁLISE DA CONTRATAÇÃO**	**VANTAGENS**	**DESVANTAGENS**
01	Banco Central do Brasil - BACEN	P.E. nº 05/2023 (82220200)	3.366.001,68	APURA Com. de Softwares e Ass. em Tecnologia da Informação S.A.	serviço contínuo sem mão de obra exclusiva	24 meses	O objeto do lote único foi composto por dois itens, sendo o primeiro a contratação de serviços de SOC (fora do escopo deste Estudo), enquanto o segundo item descreve a contratação de serviços de threat intel.	A contratação de serviços de SOC e Threat Intel dentro do mesmo objeto, parece ser uma composição operacionalmente adequada, pois há uma óbvia relação entre os dois serviços.	Ainda que os dois itens que compõem o objeto estejam relacionados, entendemos que tal relação não seja suficiente para mantê-los no mesmo lote.

02	Serviço Federal de Processamento de Dados - SERPRO	P.E. nº 196/2023 (82219967)	1.857.600,00	HARPIA Tecnologia LTDA	serviço contínuo sem mão de obra exclusiva	60 meses	Objeto composto de item único em um lote único. Foi utilizado como métrica o parâmetro "mês", indicando que o objeto será executado em parcelas.	A simplicidade do objeto é algo a ser destacado no processo. Tal simplicidade, inclusive, pode ser compatível com os objetivos do presente Estudo.	Não foi especificado item de treinamento para a devida operação da solução.
03	Tribunal Regional Eleitoral de Minas Gerais - TRE/MG	P.E. nº 63/2022 (82220747)	520.899,70	HARPIA Tecnologia LTDA	serviço contínuo sem mão de obra exclusiva	12 meses	Objeto composto por dois itens em um lote único. O primeiro deles corresponde ao serviço de inteligência, enquanto o segundo é um serviço específico (serviço de takedown) que depende do primeiro item.	O objeto referente ao serviço de cyber threat intel apresenta alguma compatibilidade com a demanda do PRODERJ, e alguns de seus elementos devem ser incorporados ao modelo a ser adotado.	O item referente ao serviço de "takedown" não é devidamente explicado no Edital. Considerando a legislação brasileira sobre o tema, questões envolvendo "notice and takedown" apresentam complexidade maior do que em outros países. Este item deveria ser melhor explicado.
04	Exército (Base Administrativa do Comando de Comunicação e Guerra Eletrônica do Exército)	P.E. nº 12/2022 (82572324)	17.500,00	HARPIA Tecnologia LTDA	Serviço de Treinamento	Evento	Evento presencial, 40 horas, contemplando material didático para turma de até 10 alunos.	O item se apresenta compatível em conteúdo e prazo, com o modelo de treinamento recorrentemente demandado pelo PRODERJ em licitações.	A modalidade presencial já não vem sendo utilizada nas licitações do PRODERJ. Todavia, nada obsta que o evento seja demandado em modalidade remota.
05	Conselho Federal de Engenharia e Agronomia - CONFEA	P.E. nº 17/2023 (82572638)	10.000,00	NETSAFE Corp LTDA	Serviço de Treinamento	Evento	Evento presencial, 40 horas, contemplando material didática para turma de 3 alunos.	O item se apresenta compatível em conteúdo e prazo, com o modelo de treinamento recorrentemente demandado pelo PRODERJ em licitações.	A modalidade presencial já não vem sendo utilizada nas licitações do PRODERJ. Todavia, nada obsta que o evento seja demandado em modalidade remota.

8.4. **Estimativa Preliminar do Valor da Contratação**

8.4.1. A estimativa preliminar do valor da contratação, visando uma análise comparativa quanto à viabilidade econômica das soluções escolhidas neste estudo técnico, considerou os parâmetros observados nos certames e contratações similares realizadas por outros órgãos da administração pública observados conforme a tabela do subtópico 8.3. deste documento.

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

8.4.3. Na tabela abaixo, constam processos relativos à contratação de solução THREAT INTEL observados na Consulta de Licitações do Portal da Transparência:

LOTE ÚNICO						
item do lote	**Idetificação**	**Fonte**	**Natureza**	**Período**	**Valor**	**valor mensal (item 1)**
1	Banco Central - P.E n 05/2023	Painel de Preços	Serviço contínuo	24 meses	720.000,00	30.000,00
	Serviço Federal de Proc de Dados - P.E n 196/2023	Painel de Preços	Serviço contínuo	60 meses	1.356.000,00	22.600,00
	Tribunal Regional Eleitoral de MG - P.E n 63/2022	Painel de Preços	Serviço contínuo	12 meses	240.000,00	20.000,00
2	em levantamento	em levantamento	em levantamento	em levantamento	em levantamento	em levantamento
3	Exército - P.E n 12/2022	Painel de Preços	Serviço por escopo	40 horas	17.500,00	-- / --
	CONFEA - P.E n 17/2023	Painel de Preços	Serviço por escopo	40 horas	10.000,00	-- / --

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

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

9. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

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

9.2. A “Solução 2” (Serviço Gerenciado) não possibilita que o Contratante exerça o pleno controle da ferramenta, nem mesmo naqueles cenários onde ele teria plenas condições de exercê-lo. Adicionalmente, teríamos ainda a desvantagem de que este tipo de contratação (serviço gerenciado) não traria muito expertise técnico para as equipes dos contratantes, pois não haveria muitas oportunidades de aprendizado para os quadros técnicos do Contratante.

9.3. A “Solução 4” (Aquisição Perpétua), além de não ser prática usual do mercado em soluções Threat Intel, ainda criaria um vínculo de dependência tecnológica que entendemos como desnecessário para tal contratação, pois ao final da garantia, o Contratante só poderia voltar a desfrutar de todas as vantagens da ferramenta caso ocorra a renovação do contrato.

9.4. Portanto, consideradas as desvantagens observadas nos modelos acima, entende-se que a “Solução 3” (Subscrição - SaaS) é a que mostra maior

benefício de ordem técnica, bem como a compatibilidade com o Sistema de Registro de Preços, corroborando a finalidade institucional do PRODERJ para a oferta de soluções tecnológicas para os demais órgãos da Administração.

10. DESCRIÇÃO DA SOLUÇÃO DE TI COMO UM TODO

Contratação de empresa de Tecnologia da Informação para o fornecimento de Serviço de Inteligência Aplicada à Segurança da Informação, abrangendo o período de 12 meses, para monitoramento constante da internet.

11. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

11.1. A solução proposta apresenta objeto único composto de três itens interdependentes, quais sejam o software (solução principal), o serviço de operação assistida do software (solução principal) e o serviço de treinamento e capacitação para operacionalização do software (solução principal). Nesse cenário, cada CONTRATANTE poderá optar pelo modelo de solução que implantará: completo ou parcial, tendo por parâmetro sua própria estrutura, seja em termos de infraestrutura, seja em termos de equipe de trabalho. Sendo certo, todavia, que a solução é uma só.

11.2. A divisão do objeto nos itens buscou, ainda, compatibilizar o objeto proposto com a lógica do Sistema de Registro de Preços, de modo que, conforme explicado, os órgãos possam contratar somente os itens que forem convenientes.

11.3. A divisão do objeto entre fabricantes distintos não se aplica, portanto, em razão da correlação intrínseca entre entre os itens do lote único, que, como já explicado, corrresponde a uma solução tecnológica e seus respectivos serviços de operação assistida e de treinamento.

11.4. Ainda que possivel a divisão do objeto, tal estratégia acarretaria prejuízos técnicos, em razão dos diversos relatórios de inteligência de ameaças fragmentados, não-coesos e, portanto, não muito úteis em termos de subsídios para uma rápida tomada de decisões que envolvam a segurança da informação do PRODERJ.

11.5. O agrupamento dos itens da contratação, portanto, é meramente natural e não apenas com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes e melhor gerenciamento do contrato.

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

11.7. A título de referência, se observa em entendimentos do Egrégio Tribunal de Constas da União, amparo ao modelo proposto neste estudo técnico:

a) Acórdão nº 861/2013 - TCU - Plenário: é lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si.

b) Acórdão nº 5.260/2011 – TCU – 1ª câmara, de 06/07/2011, “Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si”.

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

12. CONDIÇÕES GERAIS DA CONTRATAÇÃO

12.1. Modelo de execução do contrato

12.1.1. Para todos os serviços do lote único o regime de execução é o de empreitada por preço unitário.

12.2. Forma de adjudicação do objeto

12.2.1. A forma de adjudicação do objeto será MENOR PREÇO GLOBAL.

12.2.2. Para se obter o menor preço do lote deverão ser negociados os valores individualizados de cada item que o compõe, buscando também o menor preço unitário, tendo em vista que os itens se encontram agrupados em lote, meramente em razão da compatibilidade técnica/operacional intrínseca.

12.3. Dotação orçamentária

Fica dispensada a indicação de prévia dotação orçamentária no sistema de registro de preços, uma vez que será exigida tão somente quando da efetivação da respectiva contratação.

12.4. Forma e prazo de pagamento

12.4.1. O pagamento ocorrerá nas formas abaixo:

a) Para o item 1 do lote único (subscrição de software), será em parcela única a ser efetuada à vista;

b) Para o item 2 do lote único (operação assistida), será em parcelas sob demanda a serem efetuadas à vista;

c) Para o item 3 (treinamento), será em parcelas sob demanda a serem efetuadas à vista.

12.4.2. O CONTRATANTE deverá pagar o preço ao CONTRATADO, consideradas as formas previstas por item nas alíneas a, b e c, do subtópico 12.4.1, na conta-corrente de titularidade do CONTRATADO a ser indicada, junto à instituição financeira contratada pelo Estado do Rio de Janeiro.

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

12.4.4. A emissão da Nota Fiscal ou Fatura será precedida do recebimento definitivo do objeto ou de cada parcela, mediante atestação, que não poderá ser realizada pelo ordenador de despesas, conforme disposto neste instrumento e/ou no Termo de Referência, bem ainda no artigo 140, II, alínea “b”, da Lei nº 14.133/2021 e arts. 20 e 22, XXIII, do Decreto nº 48.817/2023.

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

12.4.6. O CONTRATADO deverá encaminhar a Nota Fiscal ou Fatura para o endereço indicado pelo CONTRATANTE.

12.4.7. Uma vez recebidos os documentos mencionados neste tópico, o órgão competente deverá realizar consulta ao SICAF para verificar:

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

b) Se o CONTRATADO foi penalizado com as sanções de declaração de inidoneidade ou impedimento de licitar e contratar com o poder público, observadas as abrangências de aplicação; e

c) Eventuais ocorrências impeditivas indiretas, hipótese na qual o gestor deverá verificar se houve fraude por parte das empresas apontadas no

Relatório de Ocorrências Impeditivas Indiretas.

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

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

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

12.4.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso o CONTRATADO não regularize sua situação, ressalvado o disposto no art. 121, § 3º, da Lei nº 14.133, de 2021, no art. 29 do Decreto nº 48.817, de 2023, e no Termo de Referência.

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

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

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

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

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

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

12.5. **Forma, prazo e endereço de entrega**

12.5.1. **Forma de Entrega**

12.5.1.1. A entrega do serviço de subscrição (item 1 do lote único), em parcela única, se dará de forma virtual, via e-mail cujo destinatário será informado na reunião de kick-off prevista neste documento.

12.5.1.2. A entrega do serviço de operação assistida (item 2 do lote único), em parcela sob demanda, ocorrerá de forma virtual, em modalidade remota, cuja dinâmica será informada na reunião de kick-off.

12.5.1.3. A entrega dos serviços de treinamento (item 3 do lote único), em parcela sob demanda, acontecerá através do portal de treinamentos da contratada ou que esta venha a disponibilizar.

12.5.2. **Prazo de Entrega**

12.5.2.1. O cronograma para entrega do objeto, contado em dias úteis, será conforme a tabela abaixo:

Prazo (dias)	Marco para contagem do prazo	Atividades	Responsável
2	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Emissão da "Ordem de Serviço" referente à subscrição (item 1)	CONTRATANTE
15	Publicação do extrato do contrato no Portal Nacional de Compras Públicas - PNCP	Realização da Reunião Kick-Off prevista no subtópico 5.7.2.1.	CONTRATANTE e CONTRATADA
5	Realização da reunião kick-off	Liberação do acesso da Contratante na plataforma da solução SaaS	CONTRATADA
20	Emissão da "Ordem de Serviço"	Início do Treinamento da solução	CONTRATADA
15	Realização da reunião kick-off	Configuração do escopo inicial de monitoramento que foi indicado pela Contratante na reunião de “kick-off”	CONTRATADA
30	Realização da reunião kick-off	Conclusão da configuração do escopo inicial de monitoramento na solução (entrega definitiva)	CONTRATADA
1	Conclusão da configuração do escopo inicial de monitoramento da solução	Início da prestação do serviço do item 2 (quando demandado)	CONTRATADA
2	Recebimento do Relatório de Cumprimento do Objeto, previsto no subtópico 12.9.1., inciso II.	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 12.9.3. deste documento.	CONTRATANTE

12.6. **Endereço de entrega**

12.6.1. Resguardada a forma de entrega informada no subtópico 12.5.1. deste documento, os eventuais atendimentos presenciais de suporte técnico, será realizada no endereço indicado pela Contratante.

12.6.2. No caso do PRODERJ, a entrega poderá ocorrer nos três endereços abaixo, a definir no chamado:

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

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

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

12.6.3. 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.

12.7. **Vigência contratual**

O prazo de vigência, considerados todos os itens do lote único, será de 12 (doze) meses, contados da data da divulgação no Portal Nacional de Contratações Públicas, com possibilidade de prorrogação, sucessivamente, até o máximo de 10 (dez) anos, na forma dos art. 107 da Lei nº 14.133/2021, desde que observadas as condições previstas no Contrato e mediante a celebração de termo aditivo.

12.8. **Reajuste de preços**

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

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

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

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

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

12.8.6. 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.

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

12.8.8. 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.

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

12.8.10. 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.

12.8.11. 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.

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

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

12.8.14. 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.

12.9. **Critérios de recebimento e aceitação do objeto**

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

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

II - A CONTRATADA deverá elaborar um Relatório de Cumprimento do Objeto (modelo no Anexo IV deste documento) a ser entregue à Comissão de Fiscalização de Contrato quando da entrega do serviço, para a análise antes da emissão do Termo de Recebimento Provisório. O relatório deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual. O relatório deverá estar acompanhado, conforme o serviço entregue, das seguintes informações e/ou documentos:

a) Para o serviço do item 1 do objeto: documentação que comprove o licenciamento da solução contratada, tais como número de séries, chaves, bem como dados informativos para o acionamento do suporte técnico e documentos oficiais do fabricante e documentação do produto e a disponibilização da solução;

b) Para o serviço do item 2: relatórios que informem as atividades realizadas;

c) Para o serviço do item 3 do objeto: certificados dos alunos treinados; e

d) relatórios citados no subtópico 5.7.4.12 deste documento.

12.9.2. 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.

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

12.9.4. 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.

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

12.9.6. 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.

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

12.9.8. 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.

12.9.9. 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.

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

12.10. **Participação de empresas em regime de consórcio**

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

12.10.2. 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.

12.10.3. 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.

12.10.4. 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.

12.10.5. 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.

12.10.6. 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.

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

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

12.11. **Possibilidade de participação de cooperativas**

12.11.1. Não será permitida a participação de cooperativas, tendo em vista que a natureza dos serviços e o modo como serão executados, exige subordinação jurídica entre o contratante e o contratado.

12.11.2. Diante da especificidade desta contratação, que trata do fornecimento de serviço de inteligência cibernética, englobado em lote único, bem como observado o mercado de soluções para o objeto ora proposto, composto por empresas de organização tradicional aptas a fornecer a integralidade do objeto, não se faz razoável a participação de cooperativas neste certame.

12.11.3. Saliente-se que o serviço estimado no presente estudo requer conhecimento técnico especializado na solução aplicada, não havendo no mercado cooperativa capaz de atender aos requisitos e padrões técnicos exigidos.

12.12. **Análise da possibilidade de subcontratação**

12.12.1. Não será admitida a subcontratação, sub-rogação, cessão ou transferência no todo ou em parte, em razão da composição do objeto, constituído em lote único para o fornecimento de serviços especializados.

12.12.2. 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.

12.13. **Exigência de garantia contratual**

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

12.13.2. 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, 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.

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

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

b) seguro-garantia;

c) fiança bancária; e

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

12.13.4. A garantia, qualquer que seja a modalidade apresentada pelo vencedor do certame, deverá contemplar a cobertura para os seguintes eventos:

a) Prejuízos advindos do não cumprimento do contrato;

b) Multas punitivas aplicadas pela fiscalização à contratada;

c) Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo durante a execução do contrato;

d) Obrigações previdenciárias e trabalhistas não honradas pela Contratada.

12.13.5. Caso o valor do contrato seja alterado, de acordo com o art. 124 da Lei Federal n.º 14.133/2021 a garantia deverá ser complementada, no prazo de 10 (dez) dias úteis contados da data em que a CONTRATADA for notificada, para que seja mantido o percentual de 5 % do valor do Contrato.

12.13.6. Nos casos em que valores de multa venham a ser descontados da garantia, seu valor original será recomposto no prazo de 10 (dez) dias úteis contados da data em que a CONTRATADA for notificada, sob pena de rescisão administrativa do contrato.

12.13.7. Demais termos relacionados a garantia contratual serão previstos no edital e no contrato.

12.14. **Qualificação Técnica**

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

I - O(s) atestado(s) se aplicam ao item 1 do lote único (serviço contínuo de subscrição), o qual corresponde à parcela de maior relevância ou de valor significativo para o objeto deste certame.

II - A *Comprovação da experiência mínima de 1 ano na execução do objeto, sendo aceito o somatório de atestados de períodos diferent*es, não havendo obrigatoriedade de 1 ano ser ininterrupto.

III - Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

IV - Poderá ser admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação de diferentes atestados de serviços

executados de forma concomitante, resultando na comprovação de capacidade técnico-operacional de uma única contratação.

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

12.14.2. A motivação para a comprovação de aptidão técnica, bem como o tempo mínimo 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.

12.15. **Entrega, avaliação da qualidade e aceite do objeto**

12.15.1. Os níveis dos serviços de subscrição e operação assistida (itens 1 e 2 do lote único) e do serviço de treinamento (itens 3) observarão os critérios constantes no subtópico 5.11, e consideradas as sanções previstas no subtópico 5.12, ambos deste documento.

12.15.2. A solução ofertada pelo licitante classificado em primeiro lugar será submetida a Teste de Bancada, na forma do tópico 13 deste documento.

13. TESTE DE BANCADA

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

13.2. **Prazos e condições do Teste de Bancada**

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

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

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

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

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

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

a) ID do requisito;

b) Descrição do requisito;

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

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

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

f) Outras informações necessárias.

13.2.3. Até o prazo de 5 dias úteis após a realização da reunião preparatória, será divulgada a equipe técnica que avaliará a solução durante a sessão da prova.

13.2.4. O teste será realizado no ambiente do PRODERJ, em um dos endereços abaixo mencionados a ser definido na reunião acima preparatória acima referida:

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

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

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

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

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

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

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

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

13.4. **Roteiro e critérios de avaliação**

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

13.4.2. A equipe técnica do PRODERJ considerará apto o sistema que atender aos requisitos conforme descritos no respectivo Roteiro para Teste de Bancada (Anexo II deste documento), onde cada item deverá ser preenchido, observados os critérios "atende" ou "não atende".

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

13.4.4. Após a prova será emitido, via Sistema Eletrônico de Informações, relatório descrevendo os testes realizados e a conclusão sobre a aprovação da proposta ou desclassificação bem como eventuais ocorrências ou manifestações de quaisquer dos presentes na sessão.

13.4.5. Para a solução ser considerada apta para ser contratada pela Administração, todos os requisitos de software que constam no presente documento e seu anexo de especificações técnicas, deverão ser considerados ATENDIDOS.

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

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

13.5. **Responsabilidades**

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

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

13.5.3. A disponibilização de equipamentos, sistemas, demais materiais e/ou acessórios necessários ao ambiente de demonstração durante a prova não informados pelo LICITANTE na reunião preparatória citada no subtópico 13.2.1 são de inteira responsabilidade do LICITANTE.

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

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

> Decreto Estadual nº 48.816/23, art. 21, §3º - As amostras, provas de conceito ou objetos a serem submetidos a exame de conformidade em depósito nos órgãos e entidades estaduais, sem que haja interesse dos licitantes em sua retirada, devem, após comunicação dos licitantes proprietários e perdurando o desinteresse, ser considerados como coisas abandonadas, com perda da propriedade, conforme o disposto no Art. 1.263 e inciso III do Art. 1.275 da Lei nº 10.406, de 10 de janeiro de 2002 e poderão ser incorporados ao patrimônio do Estado ou formalmente descartados.

14. ANÁLISE DE RISCO DE SOBREPOSIÇÃO DO OBJETO

14.1. Não há risco de sobreposição com outras contratações, tendo em vista que o Art. 3º, XIII, do Decreto 48.997/24, estabeleceu dentre outras diretrizes, que compete ao 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.

14.2. Diante da definição supracitada, todas as contratações de TIC são remetidas ao PRODERJ para avaliação e posterior deliberação quanto ao prosseguimento ou não do processo, o que mitiga possíveis sobreposições de contratos para o mesmo objeto.

15. DA TRANSIÇÃO E DO ENCERRAMENTO DO CONTRATO

15.1. Ao final do contrato, a Contratada deverá promover a transição contratual com vistas a não impactar a rotina do CONTRATANTE.

15.2. Entende-se por transição contratual, a transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, para servidores do CONTRATANTE ou técnicos por ele indicados, para fins de migração da solução para a eventual nova prestadora dos serviços.

16. ESTRATÉGIA DE INDEPENDÊNCIA EM RELAÇÃO À CONTRATADA / PLANO DE SUSTENTAÇÃO

Em caso de interrupção contratual, o CONTRATANTE poderá empregar, em caráter emergencial, diversas ferramentas open source, até a realização de nova contratação. Nesta hipótese, a equipe da CONTRATANTE deverá manter e administrar várias ferramentas tecnológicas, e ainda mitigar todos os alertas e eventos que elas venham a gerar.

17. RELATO DESCRITIVO DE CONTRATAÇÕES ANTERIORES DE NECESSIDADE IDÊNTICA OU SEMELHANTE

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

18. POSICIONAMENTO CONCLUSIVO

18.1. O presente Estudo Técnico Preliminar (ETP), bem como os seus anexos, consideram a necessidade de contratação do objeto formado por diversos serviços de TIC que compõem solução única, os requisitos técnicos, legais, ambientais e os do próprio negócio, o mercado em que o objeto se encontra inserido, bem como os demais requisitos necessários para a caracterização e quantificação da demanda identificada, e ainda o processo de escolha da solução que melhor se adequa à Instituição nesta oportunidade. São considerados ainda os requisitos ambientais e os aspectos legais, cabendo ressaltar que os riscos envolvidos são administráveis e os custos previstos são compatíveis e se caracterizam pela economicidade.

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

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

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

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

20. ANEXOS

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

I - Especificações Técnicas do Objeto (82347290);

II - Roteiro para Teste de Bancada (82347292);

III - Mapa de Riscos (82347633);

IV - Modelo de Relatório de Cumprimento do Objeto (82347294).

21. ASSINATURA DOS MEMBROS DA EQUIPE RESPONSÁVEL PELO ESTUDO

Monique Gonçalves Paz Diretora de Segurança da Informação ID nº 4349648-2	Rosana Alves de Andrade Gerente de Proteção de Dados e Sistemas ID nº 4347470-5	Charles Monteiro Guimarães Diretor de Patrimônio e Logística ID nº 4432892-3	Milena da Rocha Asevedo Assistente ID nº 5126815-9

Rio de Janeiro, 23 de setembro de 2024

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 23/09/2024, às 16:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/09/2024, às 16:30, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 23/09/2024, às 16:35, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 23/09/2024, às 17:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro 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 **82347287** e o código CRC **935BDB3E**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO I DO ESTUDO TÉCNICO PRELIMINAR

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. INFORMAÇÕES PRELIMINARES

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

1.2. O lote com os itens componentes do objeto se encontra na tabela do subtópico 7.4. do Estudo Técnico Preliminar.

2. CARACTERÍSTICAS GERAIS DA SOLUÇÃO

2.1. A Solução de Threat Intel deverá realizar o monitoramento através de ferramenta baseada em aplicação ou conjunto de aplicações apropriadas para esta finalidade, instaladas sobre ambiente da própria contratada, na modalidade de SaaS (Software as a Service), que possuam mecanismo de captura automatizado de informações armazenadas na surface web, deep web e dark web, sites, fóruns, blogs, aplicativos de mensagens instantâneas, mídias sociais, arquivos de logs.

2.2. A Solução de Cyber Threat Intel deve ser capaz de realizar, no mínimo, as seguintes tarefas:

I - Monitoramento e coleta automatizada;

II - Geração de alertas em tempo real;

III - Emissão de relatórios com análise de inteligência de ameaças.

2.3. A Solução não deve limitar quantidade de fontes de informação que serão utilizadas no monitoramento dos recursos pesquisados.

3. CARACTERÍSTICAS ESPECÍFICAS DOS ITENS

3.1. Subscrição de Solução Threat Intel (item 1)

3.1.1. Gerenciamento

3.1.1.1. A solução deverá ser disponibilizada ao Contratante através de plataforma web segura, acessível via Internet mediante login e senha, e possibilitar o acesso ao menos pelos navegadores Google Chrome, Mozilla Firefox e Microsoft Edge.

3.1.1.2. A contratada deverá fornecer ao Contratante direitos de acesso administrativo (credenciais/contas) para, no mínimo, 06 (seis) colaboradores.

3.1.1.3. A Solução deve permitir a configuração de ao menos dois tipos de perfis de acesso ao sistema: escrita e leitura.

3.1.1.4. A Solução deve ser capaz de realizar a autenticação de usuário por dois fatores.

3.1.1.5. A Solução deve possuir interface de fácil visualização para demonstrar os resultados das buscas por cada tipo de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, deep web e dark web).

3.1.1.6. A solução deve ter a capacidade de exibir todos os relatórios e gráficos em painel de bordo

(dashboard).

3.1.1.7. Permitir que o Contratante veja o conteúdo em seu local original, por meio de um link atrelado ao resultado da pesquisa.

3.1.1.8. Disponibilizar um ambiente para visualização das pesquisas realizadas e alertas cadastrados.

3.1.1.9. Permitir exportar qualquer pesquisa realizada de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha.

3.1.1.10. A Solução deve ter a capacidade de gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos as contas de usuários. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento e ação/pesquisa efetuada.

3.1.1.11. A Solução deverá manter a base de dados gerada pela ferramenta durante a vigência do contrato.

3.1.1.12. A Solução deve permitir acesso às suas funcionalidades por meio de API (Application Programming Interface), com suporte via interface programável API/REST.

3.1.1.13. A Solução deve possuir a capacidade de analisar dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades: visualização de perfis relacionados a palavras-chave, realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes.

3.1.2. **Monitoramento e Coleta**

3.1.2.1. A Solução deve ser capaz de realizar o monitoramento na Internet (fontes abertas, redes sociais, aplicativos de mensagens instantâneas, fóruns, blogs, surface web, deep web e dark web).

3.1.2.2. A solução deve ser capaz de realizar pesquisas automatizadas previamente cadastradas, periódicas, manuais, avulsas. A Solução não deve limitar o tamanho do escopo a ser pesquisado.

3.1.2.3. A Solução deve ser capaz de exibir os endereços ou IP nos resultados das pesquisas realizadas sobre qualquer site, inclusive os existentes na deep web e dark web.

3.1.2.4. Deve ser capaz de realizar a transcrição de áudios, imagens e vídeos capturados em aplicativos de mensagens instantâneas.

3.1.2.5. A Solução deve ser capaz de realizar pesquisa de informações nos seguintes contextos:

a) Ameaças cibernéticas;
b) Resposta a Incidentes;
c) Prevenção de perdas de dados;
d) Proteção de Marca;
e) Fraudes;
f) Domínios Web;
g) Ameaças Internas;
h) Imagem e reputação Institucionais;
i) Vazamento de dados sensíveis;
j) Vazamento de credenciais corporativas.

3.1.2.6. A solução deve ser capaz de realizar descoberta de páginas web de “phishing” ativas que utilizem nomes associados ao escopo do Contratante, a marca, identidade visual, domínios e ativos que serão protegidas.

3.1.2.7. A solução deve ser capaz de realizar validação de sites suspeitos em repositórios sob

demanda de “phishing” com validação das entidades reguladoras.

3.1.2.8. A solução deve ser capaz de identificar os endereços de correio eletrônico (e-mails) de domínios monitorados em listas de spam.

3.1.2.9. Os resultados das pesquisas devem conter, no mínimo, os seguintes campos: Contexto pesquisado, data, idioma, endereço web, conteúdo original completo.

3.1.2.10. A Solução deve permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo, no mínimo, ordenáveis por data e hora, da ocorrência mais recente para a mais antiga.

3.1.2.11. A solução deve permitir a atualização do resultado das pesquisas realizadas anteriormente com a sinalização das atualizações.

3.1.2.12. A Solução deve ter a capacidade de disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte.

3.1.2.13. Relação mínima de fontes que devem ser monitoradas:

a) Aplicativos de mensagens instantâneas: Telegram, Whatsapp e Messenger (Facebook);

b) Redes Sociais: Twitter, Facebook, Instagram, Snapchat e Linkedin;

c) Sites de busca: Google, Bing, Yahoo! e DuckDuckGo;

d) Serviços de vídeo: Youtube;

e) Ransomware: Sites de ransomware shaming;

f) Segurança cibernética: Shodan, BinaryEdge, Zone-H, Bases de CVE;

g) Lojas de aplicativos Android e Apple;

h) Outras fontes abertas: Pastebin, GhostBin, Paste24, GitHub, GitLab, Feeds RSS.

3.1.2.14. A Solução deve ser capaz de realizar a detecção de domínios de internet recentemente registrados que possam oferecer, no mínimo:

a) Riscos de serem utilizados de forma maliciosa;

b) Variações comuns de nomes;

c) Permutações de caracteres;

d) Desvio de URL (typosquatting).

3.1.2.15. Sobre o monitoramento de redes sociais:

a) A solução deve permitir a pesquisa de contas de usuários nas redes sociais por, no mínimo, nome do usuário, telefone, apelido e endereço de e-mail;

b) Possuir a busca automática de novas publicações das contas cadastradas conforme um agendamento pré-configurado;

c) Extrair metadados de cada publicação com, no mínimo: texto, endereço eletrônico, identificador e timestamp;

d) Coletar todas as publicações já feitas pela conta, mesmo que estas sejam anteriores à primeira sincronização na ferramenta;

e) Publicações já coletadas pelas aplicações deverão ser mantidas em suas bases de dados e resultados de pesquisa caso sejam excluídas de suas fontes originais.

3.1.2.16. Informar anomalias nos registros “WhoIS” dos domínios monitorados.

3.1.2.17. Detectar as páginas internas dos recursos pesquisados que estejam expostas na internet.

3.1.2.18. Identificar as vulnerabilidades dos domínios monitorados que tenham sido tornadas

públicas.

3.1.2.19. Identificar artefatos maliciosos, que remetem aos domínios protegidos.

3.1.2.20. Identificar intenções diretas de ataques aos recursos monitorados.

3.1.2.21. Identificar desfiguração de páginas (defacement).

3.1.2.22. Detectar documentos ou informações confidenciais vazadas dos recursos monitorados.

3.1.2.23. A solução deve ter a capacidade de identificar credenciais de acesso que estejam a venda em mercados negros online, permitindo buscas por no mínimo:

a) CPF;

b) Username;

c) Endereço de e-mail.

3.1.3. **Alertas e Relatórios**

3.1.3.1. A Solução deve ser capaz de configurar o envio de alertas relacionados aos monitoramentos realizados.

3.1.3.2. Os alertas deverão ser configurados, no mínimo, nos seguintes contextos:

a) Intenções de ataques a vulnerabilidades que afetem os ambientes do Contratante;

b) Intenções de ataques que tenham como objetivo os recursos pesquisados ou o seu nicho de atuação;

c) Campanhas relevantes de “hacktivismo”;

d) Atividades fraudulentas relacionadas aos recursos pesquisados;

e) Pessoas envolvidas em atividades contra os recursos pesquisados;

f) Códigos maliciosos (malwares) direcionados para os recursos pesquisados;

g) Alertar sobre a comercialização online ilegal de itens dos recursos pesquisados;

h) Discussões online que divulguem ou acompanhem informações dos recursos monitorados;

3.1.3.3. A solução deve ser capaz de emitir alertas e relatórios de inteligência sobre ameaças iminentes e tendências em períodos de tempo pré-definidos, conforme listados abaixo:

a) Online;

b) Diário;

c) Semanal;

d) Mensal;

e) Anual;

f) Determinado.

3.1.3.4. A solução deve ser capaz de gerar indicadores de comprometimento de ameaças (IOC);

3.1.3.5. Formas de envio dos Alertas:

a) Os alertas devem ser emitidos por periodicidade ou por expressão de busca;

b) Os alertas devem ser enviados à equipe do Contratante por e-mail, SMS ou aplicativos de mensageria, tais como Whatsapp ou Telegram;

c) A solução deve permitir a criação de listas de distribuição de e-mails com as informações coletadas;

d) Os alertas devem incluir, no mínimo: tipo da fonte, contexto procurado e o timestamp do momento da geração do alerta;

e) A solução deve permitir a customização dos textos dos alertas;

f) A solução deve possibilitar o envio de e-mails criptografados;

3.1.3.6. Permitir exportar todos os relatórios e gráficos de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha eletrônica e Documento Texto;

3.2. Serviço de Operação Assistida (item 2)

O catálogo de serviços para operação assistida encontra-se no subtópico 5.7.2.10. do Estudo Técnico Preliminar.

3.3. Treinamento Operacional na Solução (item 3)

Os detalhamentos sobre a realização do Treinamento na solução, abrangendo o item 1 do objeto, encontram-se no subtópico 5.2. do Estudo Técnico Preliminar.

Rio de Janeiro, 23 de setembro de 2024

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 23/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/09/2024, às 16:30, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 23/09/2024, às 16:36, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 23/09/2024, às 17:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro 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 **82347290** e o código CRC **0EA76A8B**.

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO II DO ESTUDO TÉCNICO PRELIMINAR

ROTEIRO PARA TESTE DE BANCADA

1. Será realizado o teste de bancada com o objetivo de verificar o o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante arrematante.
2. O roteiro do teste de bancada, nos termos que seguem abaixo, exigirá da licitante primeira colocada, a comprovação de que sua solução atende às especificações de maior relevância aqui elencadas.
3. As especificações selecionadas neste documento representam as características de maior impacto em relação à solução como um todo, e levam em consideração os aspectos técnicos que permitem a comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.
4. Este anexo deve ser interpretado conforme as disposições do Estudo Técnico Preliminar do qual é parte integrante e indissociável.

SOLUÇÃO DE INTELIGÊNCIA DE AMEAÇAS (THREAT INTELL)				
ITENS A SEREM AVALIADOS / CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS				
item	**ref no Anexo I**	**descrição**	**contexto do requisito**	**avaliação (atende / não atende)**
1	2.2.2.	Geração de alertas em tempo real	Características Gerais da Solução	
2	3.1.1.1.	A solução deverá ser disponibilizada ao Contratante através de plataforma web segura, acessível via Internet mediante login e senha, e possibilitar o acesso ao menos pelos navegadores Google Chrome, Mozilla Firefox e Microsoft Edge	Gerenciamento	
3	3.1.1.3.	A Solução deve permitir a configuração de ao menos dois tipos de perfis de acesso ao sistema: escrita e leitura	Gerenciamento	

4	3.1.1.5.	A Solução deve possuir interface de fácil visualização para demonstrar os resultados das buscas por cada tipo de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, deep web e dark web)	Gerenciamento	
5	3.1.1.6.	A solução deve ter a capacidade de exibir todos os relatórios e gráficos em painel de bordo (dashboard)	Gerenciamento	
6	3.1.1.7.	Permitir que o Contratante veja o conteúdo em seu local original, por meio de um link atrelado ao resultado da pesquisa	Gerenciamento	
7	3.1.1.9.	Permitir exportar qualquer pesquisa realizada de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha	Gerenciamento	
8	3.1.1.10.	A Solução deve ter a capacidade de gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todos as contas de usuários. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento e ação/pesquisa efetuada	Gerenciamento	
9	3.1.2.3.	A Solução deve ser capaz de exibir os endereços ou IP nos resultados das pesquisas realizadas sobre qualquer site, inclusive os existentes na deep web e dark web	Monitoramento e coleta	
10	3.1.2.9.	Os resultados das pesquisas devem conter, no mínimo, os seguintes campos: Contexto pesquisado, data, idioma, endereço web, conteúdo original completo	Monitoramento e coleta	
11	3.1.2.12.	A Solução deve ter a capacidade de disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte	Monitoramento e coleta	
12	3.1.2.15.1.	A solução deve permitir a pesquisa de contas de usuários nas redes sociais por, no mínimo, nome do usuário, telefone, apelido e endereço de e-mail	Monitoramento e coleta	
13	3.1.2.15.3.	Extrair metadados de cada publicação com, no mínimo: texto, endereço eletrônico, identificador e timestamp	Monitoramento e coleta	

14	3.1.3.1.	A Solução deve ser capaz de configurar o envio de alertas relacionados aos monitoramentos realizados	Monitoramento e coleta	
15	3.1.3.3.	A solução deve ser capaz de emitir alertas e relatórios de inteligência sobre ameaças iminentes e tendências em períodos de tempo pré-definidos	Monitoramento e coleta	
16	3.1.3.4.	A solução deve ser capaz de gerar indicadores de comprometimento de ameaças (IOC)	Monitoramento e coleta	
17	3.1.3.5.1.	Os alertas devem ser emitidos por periodicidade ou por expressão de busca	Monitoramento e coleta	
18	3.1.3.5.2.	Os alertas devem ser enviados à equipe do Contratante por e-mail, SMS ou aplicativos de mensageria, tais como Whatsapp ou Telegram	Monitoramento e coleta	
19	3.1.3.5.3.	A solução deve permitir a criação de listas de distribuição de e-mails com as informações coletadas	Monitoramento e coleta	
20	3.1.3.5.5.	A solução deve permitir a customização dos textos dos alertas	Monitoramento e coleta	
21	3.1.3.6.	A Solução deve possuir a capacidade de analisar dados coletados, fornecendo um painel de visualização que contemple, no mínimo, as seguintes funcionalidades: visualização de perfis relacionados a palavras-chave, realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes	Monitoramento e coleta	

Rio de Janeiro, 23 de setermbro de 2024

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 23/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/09/2024, às 16:30, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 23/09/2024, às 16:36, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 23/09/2024, às 17:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro 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 **82347292** e o código CRC **59E239D7**.

Referência: Processo nº SEI-430002/000046/2024 SEI nº 82347292

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO III DO ESTUDO TÉCNICO PRELIMINAR

MAPA DE RISCOS

1. OBJETO

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

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

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

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

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

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

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

Probabilidade (P)	15	75	150	225
	10	50	100	150
	5	25	50	75
Impacto (I)		5	10	15

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

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

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

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

Tabela de relação de riscos identificados						
Id	**Risco**	**Tipo de Risco**	**Probabilidade**	**Impacto**	**Nível de Risco (P X I)**	**Respostas aos Riscos**
R1	Não Indicação de servidores pelas áreas envolvidas no processo de aquisição para compor a Equipe de Planejamento da Contratação para elaborar a documentação necessária	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R2	Levantamento inadequado dos itens	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R3	Edital e Termo de Referência incompletos ou inconsistentes	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R4	Insuficiência de recursos orçamentários para contratação dos serviços	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R5	Não autorização de despesa para a contratação	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R6	Erro na pesquisa das quantidades necessárias para a licitação	infraestrutura	média (10)	alto (15)	150	Aceitação Ativa / Mitigar
R7	Demora na conclusão do processo licitatório, ocasionando atrasos na homologação e consequente contratação	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R8	Recusa do licitante vencedor em assinar o contrato	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa

R9	Atraso na entrega dos equipamentos (itens do objeto contratado)	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R10	Quantitativo de pessoal ou capacitação insuficiente dos agentes de fiscalização e gestão do contrato	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R11	Contratada fornecer bem fora dos padrões pretendidos	infraestrutura	baixa (5)	alto (15)	75	Aceitação Ativa
R12	Falência, insolvência, quebra contratual pela contratada	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R13	Falta de disponibilidade financeira para pagamento de despesa no prazo	infraestrutura / organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R14	Não aplicação de sanções à contratada pela Administração	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R15	Ausência de interessados na licitação como um todo ou em algum/alguns lotes do certame	organizacional	baixa (5)	alto (15)	75	Aceitação Ativa
R16	Exclusão da DSI quanto ao estabelecimento das políticas e regras para a configuração da solução.	infraestrutura	média (10)	alto (15)	150	Aceitação Ativa / Mitigar

3. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

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

RISCO 1			
Não Indicação de servidores pelas áreas envolvidas no processo de aquisição para compor a Equipe de Planejamento da Contratação para elaborar a documentação necessária.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
1.1.	Atraso na contratação;		
	Contratação em desacordo com a necessidade da Administração.		
Id	**Ação Preventiva**		**Responsável**
1.1.1.	Designar pessoal das áreas envolvidas na contratação para a composição da equipe de planejamento da contratação.		Diretores das Áreas Envolvidas
Id	**Ação de Contingência**		**Responsável**

1.1.2.	Refazer a documentação de acordo com a necessidade da Administração.	Equipe de Planejamento da Contratação

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

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

3.1.	Licitação fracassada; Contratação em desacordo com a necessidade da Administração; Prejuízo ao erário	
Id	**Ação Preventiva**	**Responsável**
3.1.1.	Revisar cuidadosamente o Edital e o Termo de Referência, de modo a verificar suas adequações.	Equipe de Planejamento da Contratação, GEA
Id	**Ação de Contingência**	**Responsável**
3.1.2.	Revogar ou anular o processo de licitação.	VPT / VPA

RISCO 4			
Insuficiência de recursos orçamentários para contratação dos serviços.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
4.1.	Inviabilidade de execução contratual.		
Id	**Ação Preventiva**		**Responsável**
4.1.1.	Prever recursos necessários no orçamento anual.		DOF
Id	**Ação de Contingência**		**Responsável**
4.1.2.	Readequar a contratação à capacidade orçamentária disponível.		Equipe de Planejamento da Contratação

RISCO 5			
Não autorização de despesa para a contratação			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta

Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	(x) Fase Preparatória ( ) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
5.1.	Inviabilidade de execução contratual.		
Id	**Ação Preventiva**		**Responsável**
5.1.1.	Prever recursos necessários no orçamento anual.		DOF
Id	**Ação de Contingência**		**Responsável**
5.1.2.	Readequar a contratação à capacidade orçamentária disponível.		Equipe de Planejamento da Contratação

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

RISCO 7

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

RISCO 8			
Recusa do licitante vencedor em assinar o contrato			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
8.1.	Impossibilidade de iniciar a execução dos serviços.		
Id	**Ação Preventiva**		**Responsável**
8.1.1.	Verificar situações que possam ensejar a inexequibilidade contratual.		AJU
Id	**Ação de Contingência**		**Responsável**
8.1.2.	Refazer os procedimentos de contratação.		GGC / AJU

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

RISCO 10			
Quantitativo de pessoal ou capacitação insuficiente dos agentes de fiscalização e gestão do contrato			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
10.1.	Falha no acompanhamento da gestão contratual		
Id	**Ação Preventiva**		**Responsável**
10.1.1.	Designar pessoal qualificado no objeto e em quantidade suficiente		PRE
	Realizar capacitação de equipe		VPA

	Realizar reuniões periódicas para atualização dos procedimentos de fiscalização contratual e compartilhamento de informações	Comissão de Fiscalização
Id	**Ação de Contingência**	**Responsável**
10.1.2.	Atribuição das atividades de gestão e fiscalização do contrato a outros servidores que já estejam capacitados	Equipe de planejamento da contratação

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

RISCO 12

Falência, insolvência, quebra contratual pela contratada.			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória ( ) Seleção do Fornecedor (x) Gestão do Contrato		
Id	**Dano**		
12.1.	Interrupção imediata do contrato		
Id	**Ação Preventiva**		**Responsável**
12.1.1.	Acompanhar as condições de habilitação da contratada, em especial quanto à qualificação econômico-financeira.		GGC
Id	**Ação de Contingência**		**Responsável**
12.1.2.	Reavaliar as empresas existentes no mercado para compra emergencial enquanto se elabora novo instrumento licitatório		GGC / DAF / GEA / DSI

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

13.1.2.	Solicitar repasse de recurso ao Tesouro para realizar pagamento no prazo.	DOF / GOF

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

RISCO 15			
Ausência de interessados na licitação como um todo ou em algum/alguns lotes do certame			
Probabilidade:	(x) Baixa	( ) Média	( ) Alta
Impacto:	( ) Baixa	( ) Média	(x) Alta
Fase Impactada:	( ) Fase Preparatória (x) Seleção do Fornecedor ( ) Gestão do Contrato		
Id	**Dano**		
14.1.	Licitação deserta ou fracassada Falta do fornecimento pretendido		

Id	Ação Preventiva	Responsável
14.1.1.	Realização de pesquisa de preços ampla	Equipe de planejamento
Id	**Ação de Contingência**	**Responsável**
14.1.2.	Repetição do certame ou contratação direta, na forma do artigo 75, III, da Lei nº 14.133/2021, se o certame, justificadamente, não puder ser repetido sem prejuízo para a Administração	VPA

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

Rio de Janeiro, 23 de setembro de 2024

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 23/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/09/2024, às 16:30, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 23/09/2024, às 16:37, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 23/09/2024, às 17:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro 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 **82347633** e o código CRC **8315BFAD**.

Referência: Processo nº SEI-430002/000046/2024 SEI nº 82347633

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

Governo do Estado do Rio de Janeiro

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

Vice Presidência de Tecnologia

ANEXO IV DO ESTUDO TÉCNICO PRELIMINAR

MODELO DE RELATÓRIO DE CUMPRIMENTO DO OBJETO

(para atendimento do subtópico 12.9.1, inciso II do ETP

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

(logo da empresa)

1. IDENTIFICAÇÃO			
Contrato nº			
Contratada		**CNPJ**	
nº da OS/AF		**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 Autorização 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

Rio de Janeiro, 23 de setermbro de 2024

Documento assinado eletronicamente por **Monique Goncalves Paz**, **Diretora**, em 23/09/2024, às 15:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Charles Monteiro Guimarães**, **Diretor**, em 23/09/2024, às 16:30, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 23/09/2024, às 16:37, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Marco Antonio de Andrade**, **Assessor Chefe**, em 23/09/2024, às 17:18, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro 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 **82347294** e o código CRC **2725F4B3**.

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