TERMO DE REFERÊNCIA

REGISTRO DE PREÇOS PARA PRESTAÇÃO DE SERVIÇO DE CENTRO DE OPERAÇÃO DE SEGURANÇA (SOC) AVANÇADO, REMOTO, PARA MONITORAMENTO CONTÍNUO POR 24 HORAS X 7 DIAS PELO PRAZO DE 24 MESES, COM EQUIPE DE SEGURANÇA REMOTA (CSIRT) DE NÍVEL 1, 2 E 3 PARA GESTÃO DE EVENTOS, DETECÇÃO DE AMEAÇAS, INCIDENTES, RISCOS E ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA A EVENTOS/INCIDENTES DE SEGURANÇA NO DATACENTER DA IPLANRIO, INCLUINDO TODOS OS RECURSOS PARA EXECUÇÃO DO SERVIÇO DE ACORDO COM AS ESPECIFICAÇÕES E DETALHAMENTOS DESTE TERMO.

JUNHO/2025

1. DO OBJETO

1.1 Registro de Preços com o objetivo de contratação de empresa para prestação de serviço de Centro de Operação de Segurança (SOC) avançado, remoto, para monitoramento contÍnuo por 24 horas x 7 dias pelo prazo de 24 meses, com equipe de segurança (CSIRT) remoto de nível 1, 2 e 3 para gestão de eventos, detecção de ameaças, resposta a incidentes, gestão de riscos, simulação de ameaças, orquestração e automação de respostas de segurança a eventos/incidentes de segurança do Datacenter da IPLANRIO, incluindo todos os recursos necessários a execução do serviço descrito neste documento, que devem ser integrar ao ambiente da CONTRATANTE.

1.2 O objeto descrito neste Termo de Referência é caracterizado como comum, sendo cabível a utilização da modalidade de licitação denominada Pregão, na sua forma eletrônica, tendo em vista que foi objetivamente definido neste documento por meio de especificações usuais e amplas do mercado.

1.3 Trata-se de objeto disponível em mercado próprio, fornecido habitualmente, independentemente da demanda da Administração, de forma padronizada, sem a exigência de atendimento de qualquer especificidade ou variantes de adequação.

1.4 Trata-se de serviço de caráter continuado sem dedicação exclusiva de mão de obra.

2. DA JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO

A IPLANRIO busca aprimorar suas operações de continuidade dos serviços de Tecnologia da Informação e Comunicação (TIC) e agilizar a resposta a eventos e comportamentos anômalos que possam afetar o ambiente de produção. Após o último ataque hacker ocorrido no ano de 2022, que deixou diversos serviços de TI indisponíveis, afetando as atividades da Prefeitura da Cidade do Rio de Janeiro e prejudicando os cidadãos, é crucial a implementação de um Centro de Operações de Segurança para monitoramento contínuo, 24 horas por dia, todos os dias da semana. Essa medida visa detectar anomalias no ambiente e tomar ações proativas para conter e impedir a propagação de incidentes, aumentando assim a credibilidade e confiança nas soluções de TI.

O monitoramento em tempo real proporciona maior visibilidade e, quando correlacionado com eventos de segurança, permite ações proativas e emergenciais para impedir ameaças e ataques resultantes de falhas e exposições de riscos. A centralização dos logs e eventos de todos os ativos de TI, incluindo servidores, equipamentos de rede, sistemas de negócios e ferramentas de segurança, aliada à inteligência artificial e aprendizado de máquina, é essencial para uma resposta eficaz a incidentes de segurança.

A equipe da IPLANRIO, atualmente reduzida, carece de conhecimentos avançados para o desenvolvimento de conectores, APIs, customizações de play books e integrações com soluções existentes no Datacenter. Portanto, é imperativo dispor de uma equipe dedicada para monitorar eventos de segurança e implementar soluções de Detecção e Resposta aos Incidentes de Segurança para centralização, agregação, correlação e tratamento de eventos.

Dessa forma, a contratação desse serviço é necessária para reduzir a exposição aos riscos do ambiente, implementar ações proativas de proteção e reagir de forma eficiente a incidentes de segurança. Optou-se pela prestação do serviço em site remoto, utilizando soluções de segurança, garantindo a disponibilidade dos recursos necessários e o monitoramento contínuo do ambiente do Datacenter da IPLANRIO, com equipes dedicadas para detectar, notificar, agir e restabelecer a segurança de nossos sistemas críticos.

São objetivos pretendidos com a contratação:

1) Melhorar a segurança do Datacenter, garantindo a proteção dos ativos e informações do ambiente tecnológico da IPLANRIO por meio de monitoramento avançado, detecção proativa de ameaças e resposta eficaz a incidentes de segurança;
2) Reduzir o tempo de detecção e resposta a incidentes, estabelecendo metas para diminuir o tempo necessário para detectar e responder a eventos e incidentes de segurança, visando minimizar o impacto potencial de ameaças cibernéticas;

3) Aprimorar a gestão de riscos, implementando processos e práticas para avaliação contínua dos riscos de segurança do Datacenter e adoção de medidas preventivas e corretivas adequadas para mitigar esses riscos;

4) Promover a conformidade com regulamentações e padrões de segurança, assegurando que o Datacenter da IPLANRIO esteja em conformidade com as regulamentações e padrões de segurança aplicáveis, como a LGPD (Lei Geral de Proteção de Dados) e normas internacionais como ISO 27001;

5) Aumentar a eficiência operacional, implementando soluções de automação e orquestração de respostas de segurança para otimizar os processos de gestão de eventos e incidentes, reduzindo a carga de trabalho manual e permitindo uma resposta mais rápida e eficiente; e

6) Aprimorar a segurança do Datacenter da IPLANRIO, garantindo uma abordagem proativa na identificação e mitigação de ameaças cibernéticas, a partir de simulações de ataques controladas para identificar potenciais vulnerabilidades no ambiente da IPLANRIO, visando fortalecer as defesas contra possíveis brechas de segurança.

3. DA DESCRIÇÃO DOS SERVIÇOS

3.1. A prestação do serviço compreende os seguintes requisitos, quantidades e prazos estimados, conforme as especificações técnicas:

ITEM	DESCRIÇÃO	Tipo	QTDE
1	IMPLANTAÇÃO DA SOLUÇÃO CONTRATADA	Serviço	1
	SERVIÇO DE CENTRO DE OPERAÇÃO DE SEGURANÇA (SOC) AVANÇADO, REMOTO, PARA MONITORAMENTO CONTÍNUO POR 24 HORAS X 7 DIAS PELO PRAZO DE 24 MESES, COM EQUIPE DE SEGURANÇA REMOTA DE NÍVEL 1, 2 E 3 PARA GESTÃO DE EVENTOS, DETECÇÃO DE AMEAÇAS,	Serviço	24 meses

ITEM	DESCRIÇÃO	Tipo	QTDE
	INCIDENTES, RISCOS E ORQUESTRAÇÃO, PARA RESPOSTAS A EVENTOS/INCIDENTES DE SEGURANÇA CIBERNÉTICA.		
3	SERVIÇO DE TREINAMENTO EM PLATAFORMA DETECÇÃO E RESPOSTA A INCIDENTES DE SEGURANÇA	Serviço	1

Tabela do Objeto do Termo de Referência

3.2. A prestação do serviço de SOC avançado será executado pelo período de 24 horas x 7 dias da semana, pelo prazo de 24 (vinte e quatro) meses, de acordo com as especificações deste documento;

3.3. Os serviços técnicos especializados de Segurança de TI, foram categorizados, e detalhados da seguinte forma:

- Implantação de serviço (Item 1 da tabela)
- Assessment de segurança (Item 2 da tabela)
- Teste de Invasão (Item 2 da tabela)
- Detecção e Resposta a Incidentes (Item 2 da tabela)
- Cibervigilância (Item 2 da tabela)
- Simulação de ameaças (Item 2 da tabela)
- Treinamento nas soluções propostas (Item 3 da tabela)

3.4. VISTORIA TÉCNICA

3.4.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por responsável técnico da CONTRATANTE designado para esse fim, de segunda à sexta-feira, das 09 horas às 18 horas, mediante agendamento prévio pelo email dop.gsc@prefeitura.rio.

3.4.2. Poderá solicitar reunião virtual para esclarecimentos de dúvidas, e demais detalhamentos para composição da proposta de preços, com equipe técnica da CONTRATANTE designada para esse fim, de segunda à sexta-feira, das 09 horas às 18 horas, mediante agendamento prévio.

3.4.3. Considerando a complexidade do ambiente tecnológico existente no Datacenter da IPLANRIO, a vistoria presencial ou reunião virtual é fortemente recomendada.

3.4.4. A vistoria informará as tarefas, projetos, procedimentos, condições e eventuais dificuldades para a prestação dos serviços, bem como informações sobre a Política de Segurança da Informação e Datacenter para compor a formulação da Proposta de Preços.

3.4.5. O ambiente tecnológico será apresentado e detalhado aos interessados em data agendada, sob a assinatura do Termo de Privacidade e Confidencialidade (Anexo II) e Termo de Ciência e Vistoria (Anexo III)

3.4.6. Para a vistoria, o licitante ou o seu representante legal, deverá atentar ao prazo para vistoria, estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria ou solicitação em e-mail corporativo, identificando o nome da organização

3.5. INFRAESTRUTURA DOS SOCS

3.5.1. A prestadora de serviço deverá possuir, pelo menos, 2 (dois) centros de operação de segurança (SOC), sendo pelo menos 1 (um) deles no Estado do Rio de Janeiro, redundantes entre si e distantes, no mínimo, 50km geograficamente um do outro.

3.5.1.1. Estes ambientes já devem estar em pleno funcionamento na data da diligência, redundantes, de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados;

3.5.1.2. Os Centros de Operação de Segurança utilizados para a prestação do serviço deverão possuir a certificação ISO/IEC 27001 vigente, emitida em nome da CONTRATADA por organização independente acreditada pelo Inmetro ou por autoridade equivalente globalmente reconhecida;

3.5.2. A CONTRATADA deverá estabelecer um canal de dados dedicado para interligação entre os SOCs primário e secundário ao Datacenter da CONTRATANTE;

3.5.3. Toda a infraestrutura necessária para adequada execução do serviço, hardware, armazenamento, ferramentas e licenciamento de software e mão de obra capacitada são de responsabilidade da CONTRATADA;

3.5.4. Deverá notificar com antecedência, toda e qualquer, indisponibilidade ou manutenção programada, e as ações de mitigação para que não haja interrupção do serviço continuo a ser prestado;

3.5.5. Os Centros de Operações de Segurança da CONTRATADA deverão possuir processos implementados que garantam a segurança das informações da CONTRATANTE. Estes processos devem estar certificados pelas normas ABNT NBR ISO/IEC 27001.

3.5.6. A CONTRATADA deverá disponibilizar linha telefônica para abertura e acompanhamento de chamados;

3.5.7. A CONTRATADA deverá possuir um gerador de energia para as áreas privativas para atender as demandas dos Centros de Operações de Segurança;

3.5.8. A CONTRATADA deverá possuir controle de acesso por biometria para os Centros de Operações de Segurança;

3.5.9. A CONTRATADA deverá possuir circuito interno de registro e gravação de imagem para os Centros de Operações de Segurança;

3.5.10. Os Centros de Operações de Segurança da CONTRATADA devem possuir múltiplas conexões independentes para acesso à Internet. Cada conexão para acesso à Internet deve ser capaz de, isoladamente, suportar a operação, de forma que a falha de uma conexão isoladamente não afete o funcionamento da operação;

3.5.11. Todas as características exigidas nesse item para os Centros de Operações de Segurança poderão ser confirmadas em diligência presencial.

3.6. EQUIPE DE SOC

3.6.1. Equipe de Security Operation Center - SOC, deve ser formada por profissionais qualificados para operação e monitoramento de eventos, detecção e alertas de segurança, esta equipe deve ser composta por um gerente e analistas de segurança com experiência mínima de 02 (dois) anos em SOC, e ter no mínimo

02 (duas) das seguintes certificações de acordo com função a ser desempenhada:

3.6.1.1. Gerente de SOC - Certificação Information Security Manager (CISM) e/ou EC-council CCISO e/ou ISC2 CISSP (Certified Information Systems Security Professional).

3.6.1.2. Líder Técnico de segurança de CSIRT: certificação CompTIA Security+ e/ou CompTIA Cysa+ e/ou ISFS (Information Security Foundation) e/ou GIAC GSEC.

3.6.1.3. Analista de segurança de CSIRT SR: certificação CompTIA Security+ e/ou CompTIA Cysa+ e/ou ISFS (Information Security Foundation) e/ou EC-Council CEH.

3.6.1.4. Analista de segurança de CSIRT PL: certificação Certified CompTIA Security e/ou CompTIA Cysa+ e/ou ISFS (Information Security Foundation).

3.6.1.5. Analista de segurança de CSIRT JR: certificação Certified CompTIA Security e/ou ISFS (Information Security Foundation).

3.6.2. Os profissionais da CONTRATADA devem possuir habilidades comportamentais, capacidade de trabalho em grupo, capacidade de escrita e de tomada de decisão de seguir processos e normas;

3.6.3. Durante a execução dos serviços, a CONTRATADA deverá disponibilizar profissionais, com formação de nível superior, graduados na área de Tecnologia da Informação, para coordenar e atuar nas atividades inerente ao serviço a ser prestado;

3.6.4. A equipe da CONTRATADA alocada para execução dos serviços devem ter experiência e certificação nas soluções propostas;

3.6.5. A equipe da CONTRATADA alocada na execução dos serviços deve possuir conhecimento sobre privacidade de dados, normas e padrões ISO’s 27001, 27002 e demais frameworks de “CIS Controls”;

3.6.6. O atendimento deverá ser realizado integralmente de forma remota e não será exigido a dedicação exclusiva de profissionais na execução dos serviços de analista de segurança de SOC, desde que a plataforma de gestão de segurança esteja configurada e se integre com todos os ativos de TI descritos neste documento. Já em caso de um cenário definido de crise, pode ser solicitada a dedicação exclusiva dos especialistas de segurança necessários ao

atendimento, inclusive com a possibilidade desse atendimento se dar de forma presencial;

3.6.7. As ações conjuntas de infraestrutura com a equipe de segurança, devem atender as melhores práticas, visando a implantação de melhorias, automação do processo de operação;

3.6.8. A equipe da CONTRATADA deve atuar em conformidade com a política de segurança da IPLANRIO;

3.6.9. Todos os profissionais envolvidos na prestação de serviço devem assinar e registrar o TERMO DE PRIVACIDADE E RESPONSABILIDADE DE SERVIÇO, sendo responsabilidade da CONTRATADA a atualização dos dados, bem como a revogação de acessos de colaboradores desligados do quadro da empresa;

3.6.10. Somente mediante, entrega do TERMO DE PRIVACIDADE E RESPONSABILIDADE DE SERVIÇO, pelos colaboradores, poderão ter autorização de acesso a senhas com privilégios para acesso aos serviços alvo deste documento.

3.6.11. A CONTRATADA deverá manter, atualizar e revogar todas as credenciais e permissão de acesso da equipe alocada aos recursos da CONTRATANTE

3.6.12. A função de gerente deve ser dedicada a prestação de serviços pertinentes a aos especificados neste termo, de forma a ser o interlocutor entre as equipes de SOC, de forma a realizar a gestão dos serviços contratados, devendo atuar em horário comercial e de forma presencial no SOC;

3.6.13. As responsabilidades atribuídas a experiência de perfil de profissional:

- Nível 1 (N1): analistas de segurança responsáveis por monitorar alertas de segurança, realizar análises preliminares e encaminhar incidentes mais complexos para níveis superiores.
- Nível 2 (N2): analistas de segurança com habilidades mais avançadas, capazes de realizar investigações mais profundas e responder a incidentes de maior complexidade.
- Nível 3 (N3): analistas de seguranças altamente especializados e com experiências em ameaças altamente sofisticadas, que requerem análises forenses e desenvolvimento de estratégias avançadas de resposta a incidentes.

3.7. ATIVOS DE TI A SEREM PROTEGIDOS

3.7.1. Os ativos de TI da CONTRATANTE, compreendem servidores com sistemas operacionais Windows, Linux, Virtualização VMware e Citrix, servidores de WEB, servidores de banco de dados, plataforma de Kubernetes, appliance, firewall (IPS/IDS/ANTI-SPAM/ANTI-BOT/URL/Filter/ANTI-VIRUS), roteadores, squid proxy, soluções em cloud de antivírus (EDR/XDR), microssegmentação de tráfego, gestão de vulnerabilidades, DNS/Bind, balanceadores de cargas (afm, asm, ltm), servidores de diversas funções, e outros ativos de rede (roteadores e switches) relevantes, conforme a tabela abaixo:

Ativos de TI	Qtde	Unidade	Tráfego GB	Size Log/dia
Servidores Windows	295	Hosts		1.000GB
Servidores Linux	587	Hosts		1.500GB
Servidores de Virtualização	149	Hosts		1.000GB
SQUID Proxy	10	Hosts	10 Gbps	1.000GB
Controladores de domínios ~11.000 usuários e 10.500 desktops	4	Hosts		1.000GB
TOTAL DE ATIVOS	1045	Hosts		
Firewall	4	Devices	60 Gbps	
WAF	2	Devices	60 Gbps	
Roteadores de borda	6	Devices	600 Gbps	2.000GB
Switches cores	20	Devices	200 Gbps	1.000GB
Switchs SAN	10	Devices	100 Gbps	1.000GB
Links de dados WAN + roteador	4	Circuitos	14 Gbps	4.000GB

Ativos de TI	Qtde	Unidade	Tráfego GB	Size Log/dia
Link de dados LPCD + roteador	1500	Circuitos	30 Gbps	1.500GB
TOTAL DE NETWORKS	1552		1064 Gbps	
Microssegmentação em Cloud	1500	Hosts	2 Gbps	
Antivírus EDR/XDR em Cloud	22000	Devices	2 Gbps	
Gestão de vulnerabilidades em Cloud	1500	Hosts	2 Gbps	
TOTAL SAAS			6 Gbps	
Diretório de nomes (AD+OpenLDAP+Novell)	60000	Nomes		1.000GB
Domínios de nomes (zonas)	100	Zonas		1.000GB
Banco de dados	1000	Databases		1.000GB
Aplicações WEB	1400	Apps		1.400GB
Aplicações Kubernetes	100	Pods		1.000GB
Dispositivos de backup	6	Devices		1.000GB
TOTAL		-	-	20.000 GB

Tabela – Ativos de TI protegido

3.7.2. Para fins de dimensionamento da capacidade da plataforma de detecção e resposta a incidentes, deverá ser previsto acréscimo de 10% do ambiente a cada ano do contrato, sem ônus a CONTRATANTE:

- Ano 1: 23.552;
- Ano 2: 23.552 + 2.355 = 25.907

3.7.3. É de responsabilidade da CONTRATANTE, fornecer e disponibilizar acesso ao catálogo de serviços e seus componentes a contratada, através de sistema de ITSM da CONTRATANTE;

3.7.4. A contratada deverá manter, atualizar revisar os agentes de coleta, de forma a garantir a entrega do serviço;

3.7.5. É de responsabilidade da CONTRATADA instalar, configurar, coletar, integrar e capturar todos os eventos, logs, tráfegos de rede e demais dados relevantes para integração a solução de gestão de segurança centralizada da CONTRATADA;

3.7.6. Todos as credenciais e permissão de acesso serão concedidos a CONTRATADA, mediante cumprimento de todas as exigências da Política de Segurança da CONTRATANTE;

3.8. FERRAMENTAS FORNECIDAS

3.8.1. Não serão aceitas ferramentas gratuitas, desenvolvidas pela, ou para, própria LICITANTE e/ou baseadas em softwares projetados para uso genérico, devendo estas serem providas por fabricantes amplamente consolidados no mercado;

3.8.2. Todas as ferramentas fornecidas como parte das soluções devem contar com serviços plenos de sustentação, conforme a seguir;

3.8.3. A sustentação, administração, operação, suporte técnico e atualização das Soluções informatizadas fornecidas pela CONTRATADA, bem como qualquer outra que se faça necessária para o pleno e adequado atendimento ao escopo e requisitos, serão serviços de natureza continuada de responsabilidade da CONTRATADA;

3.8.4. As ferramentas utilizadas devem ser providas em infraestrutura da CONTRATANTE, ou em ambiente de computação em nuvem pública adequado;

3.8.4.1. Se houver a necessidade de implantação de controladores, concentradores, coletores, sensores, agentes, conectores, equipamentos dedicados (appliances) e qualquer outro recurso de hardware e software local na infraestrutura interna da CONTRATANTE, a CONTRATADA deve fornecer e sustentar todos os recursos necessários e ser responsável pelo seu fornecimento, implantação, instalação, configuração, sustentação, atualização, administração e operação, sem custo adicional.

3.8.4.2. A CONTRATANTE disponibilizará, nos casos de instalação de hardware, tão somente a estrutura física básica de data center ou sala de dados: espaço físico e fornecimento de energia elétrica e refrigeração.

3.8.5. Todas as Soluções Informatizadas devem possuir os serviços de licenciamento ou subscrição, garantia, suporte técnico e atualização oficiais do fabricante, com níveis de serviço adequados e compatíveis com os dos serviços envolvidos, que devem estar contratados e disponíveis a partir da implantação da respectiva solução e durante toda a vigência do contrato;

3.8.6. As Soluções Informatizadas devem atender às especificações técnicas do objeto durante o prazo de vigência do contrato;

3.8.7. As Soluções Informatizadas não podem constar, no momento da apresentação da proposta comercial, em listas de end-of-sale, end-of-support, end-of-life ou similares do fabricante, e não podem ter previsão de descontinuidade de fornecimento, suporte ou vida pelo menos até o fim da vigência prevista para o contrato;

3.8.8. As Soluções Informatizadas devem ser instaladas em sua versão mais estável e atualizada;

3.8.9. A CONTRATADA deverá cumprir todos os termos e condições do contrato de licenciamento dos respectivos fabricantes das Soluções Informatizadas, cuidando do adequado dimensionamento quantitativo e qualitativo das licenças necessárias para a prestação dos serviços e aderência ao ambiente da CONTRATANTE, mantendo a conformidade com os direitos de propriedade intelectual;

3.8.10. A CONTRATADA deve comprovar, na contratação e durante toda a vigência do contrato, que tenha, junto ao fabricante de cada ferramenta das Soluções informatizadas, amplo e irrestrito acesso aos recursos e serviços de

apoio técnico bem como à plenitude de capacidades e efetividade da ferramenta, prestados diretamente pelo fabricante, como centros e laboratórios de inteligência, investigação, diagnóstico, análise e automação, dentre outros aplicáveis;

3.8.11. A CONTRATADA assegurará garantia integral e perfeito funcionamento das Soluções Informatizadas pelo período de vigência do contrato.

3.8.12. A CONTRATADA assegurará que todos os equipamentos dedicados (appliances) e qualquer outro recurso de hardware e software local instalados no ambiente da CONTRATANTE, deverão ter seus direitos de propriedade transferidos integralmente para a CONTRATANTE ao final da vigência contratual;

4. ESCOPO DO SERVIÇO

4.1. PRINCIPAIS ATIVIDADES DO SOC

4.1.1. A prestação dos serviços compreende como principais atividades:

4.1.1.1 Elaborar plano de implantação, processo de trabalho, apresentar cronograma para configuração do ambiente da CONTRATADA para integração a solução de segurança da CONTRATANTE

4.1.1.2 Fazer a gestão de eventos e correlacionamento de dados de segurança, contemplando apoiar com procedimento para as instalações de agentes coletores, desenvolvimento de casos de uso para detecção de eventos maliciosos, investigação de segurança e recomendar ações para mitigação dos eventos no futuro;

4.1.1.3 Os dados coletados, devem ter tratamento, quanto a compactação, agregação e deduplicação para envio e armazenamento em Solução de gestão de segurança da CONTRATADA;

4.1.1.4 Realizar o monitoramento, análise de vulnerabilidades, ameaças, alertas de segurança e ataques cibernéticos no ambiente;

4.1.1.5 Avaliar riscos de segurança e atuar com medidas proativas, corretivas e emergenciais;

4.1.1.6 Elaborar e manter um plano de resposta a incidentes e plano de comunicação;

4.1.1.7 Agir de forma proativa e/ou imediata, em incidentes de alta severidade, de acordo com o plano de resposta a incidentes a ser elaborado pelos responsáveis da CONTRATADA e CONTRATANTE, visando a contenção, contorno ou solução definitiva do incidente de segurança;

4.1.1.8 Operação e resposta a requisições, resolução a incidentes conhecidos e agir de forma proativa para reduzir os riscos de interrupção de serviços da CONTRATANTE;

4.1.1.9 A CONTRATADA deverá manter equipe de CTI (Cyber Threat Intelligence), com metodologias baseadas no framework MITRE ATT&CK, realizando investigações proativas e entregando relatórios periódicos de atividades suspeitas não detectadas por regras convencionais.

4.1.1.10 Realizar operações rotineiras de forma automáticas e manuais com técnicas de Threat Hunting para descoberta de ameaças e novas tendências baseadas em inteligência de ameaças no ambiente;

4.1.1.11 Apoiar e atuar em operações de Segurança de Redes, Segurança de workstation e servidores, Segurança em Banco de dados e Segurança de Aplicações;

4.1.1.12 Orquestração, automação de resposta a eventos e incidentes de segurança com risco em potencial;

4.1.1.13 Reduzir as atividades repetidas, mitigar os alertas de falso-positivos e priorizar os alertas relevantes;

4.1.1.14 Monitorar e atuar de forma a avaliar o tráfego de borda (externo e interno) suspeito e malicioso e demais dispositivos de rede;

4.1.1.15 Aplicar a Inteligência de proteção contra-ataques cibernéticos;

4.1.1.16 Registrar incidentes, problemas, vulnerabilidades e demais eventos relevantes em solução de ITSM, a comunicação deve ser efetiva com os responsáveis da CONTRATANTE, assegurando que as informações necessárias estão devidamente registradas no chamado;

4.1.1.17 Envolver os responsáveis da CONTRATANTE durante a investigação e diagnósticos do incidente crítico;

4.1.1.18 Posicionar de forma proativa e iniciador do incidente, sobre o ciclo de vida de incidente, intervir junto as equipes envolvidas para sanar os

incidentes, com ações de alinhamento e planos para que os indicadores de qualidade sejam atendidos conforme estabelecido, e se necessário façam o escalonamento hierárquico;

4.1.1.19 Passagem de conhecimento sobre segurança da informação, com planos, programas, workshops e demais informações sobre o tema de segurança, agregando conhecimento;

4.1.1.20 Realizar serviços técnicos especializado em segurança para auxiliar nos problemas detectados de segurança e nas ferramentas de defesa cibernéticas;

4.1.1.21 Integrar e monitorar de forma centralizada, incluindo todas as demais ferramentas de segurança existente no ambiente da CONTRATANTE, mediante uso de Open XDR ou Nativo XDR, API REST/XML, scripts e plug-ins para obtenção de dados das origens para armazenamento e centralização dos eventos e aplicação de inteligência na detecção de ameaças na solução de gestão de segurança da CONTRATADA;

4.1.1.22 Elaborar mensalmente, relatórios de riscos, atividades realizadas, incidentes ocorridos e demais fatos relevantes ocorridos no período, para os indicadores:

- Quantitativo de eventos correlacionados;
- Quantitativo de incidentes abertos;
- Quantitativo de solicitações por tipo de tecnologia;
- Quantitativo de regras de correlacionamento;
- TOP 10 – Regras de correlacionamento;
- TOP 10 – Tipos de ataques;
- Status da operação de cada serviço;
- Estatísticas de bloqueio de ataques;
- Estatística de Triagem e Encaminhamento de Alertas;
- Estatística de Tratamento e Resposta a incidentes;

4.1.1.23 Disponibilizar painel/dashboards de monitoração de segurança, para acompanhamento em tempo real pela CONTRATANTE;

4.1.1.24 Apoiar na definição e projetos de gestão de riscos e na elaboração de planos de continuidade e recuperação de serviços críticos de TI;

4.1.1.25 Deverá atuar de forma proativa, reativa, planejada e programada para garantir que os serviços críticos da CONTRATANTE não sofram ataques cibernéticos ou que sejam reduzidos os impactos negativos a organização.

4.2 SERVIÇOS DE GESTÃO DE SEGURANÇA

4.2.1 Deverá ser prestado pelo profissional de perfil de gerente, para gestão dos grupos de serviços de SOC;

4.2.2 Atuar em horário comercial, sendo substituído fora deste horário por profissional com capacitação igual ou superior.

4.2.3 Deverá interagir com os profissionais indicados da CONTRATANTE, durante a vigência do contrato;

4.2.4 Deverá manter atualizados a lista de profissionais alocados e os respectivos termos de privacidade e responsabilidade, para revogação de acessos e permissões, quando necessário;

4.2.5 Desenvolver fluxo de comunicação, conforme prioridade e tipo de incidente;

4.2.6 Criação de Matriz RACI, estabelecendo os papéis dos envolvidos no tratamento e resposta a incidentes;

4.2.7 Elaboração de relatórios mensais sobre as atividades realizadas, reporte de incidentes, vulnerabilidades, com as devidas evidências das ferramentas e softwares de gestão da CONTRATADA;

4.2.8 Todos os eventos de vulnerabilidades, riscos e incidentes devem ser registrados em ferramenta de ITSM da CONTRATADA;

4.2.9 Deverá propor ações de melhorias e recomendações de segurança organizacional;

4.2.10 Deverá notificar qualquer anomalia ou evento que esteja ocorrendo no ambiente, dentro dos prazos acordados;

4.2.11 Deverá apoiar no projeto de gestão de riscos, durante todas as fases; definição, mapeamento e revisão do processo;

4.3 IMPLANTAÇÃO DO SERVIÇO

4.3.1 A contratada deverá disponibilizar um gerente de projeto para controlar as entregas previstas durante o plano de implantação do serviço.

4.3.2 Deverá ser realizado reunião de alinhamento entre a CONTRATADA e CONTRATANTE, em até 10 (dez) dias úteis, para descrever o plano de atividade, cronograma de execução e início da operação do SOC e CSIRT, contendo os principais tópicos:

- Apresentação dos gerentes e canais de comunicação
- Validação dos profissionais a serem alocados (experiência e certificações)
- Apresentação dos gerentes alocados seus papéis e responsabilidades, dados de contato (e-mail / telefone celular)
- Lista de profissionais alocados, seus papéis e responsabilidades, dados de contato (Email, telefone e celular)
- Entrega dos termos de privacidade e responsabilidade
- Ativação do circuito de dados dedicados para interligação entre os sites da CONTRATADA e CONTRATANTE
- Definição macro do processo de trabalho SOC/CSIRT
- Apresentação da ferramenta de gestão de segurança
- Apresentação da ferramenta de ITSM
- Passagem de conhecimento e acessos aos recursos alvos de proteção deste documento
- Entrega de painel de monitoramento em tempo real
- Aceite de Início de operação do SOC

4.3.3 A implantação do serviço, contempla o planejamento, instalação e configuração de agentes e integrações com as soluções existentes da CONTRATANTE, e deverá ser executada em até 60 (sessenta) dias corridos, após a aprovação do plano de implantação entre ambas as partes;

4.3.4 A contratada será responsável por sugerir a estratégia de segurança a ser abordada;

4.3.5 A priorização de embarque de ativos deve ser validada em conjunto com a contratante.

4.4 ASSESSMENT DE SEGURANÇA

4.4.1 A CONTRATADA deverá realizar um Risk Assessment (Análise de Riscos e Controles Cibernéticos) utilizando como referência os frameworks NIST CSF 2.0, CIS Controls versão 8.1 e a norma ABNT/IEC ISO 27001.

4.4.2 A crescente sofisticação das ameaças cibernéticas, o aumento de ataques direcionados e a evolução regulatória exigem uma abordagem estruturada para identificação, avaliação e tratamento de riscos cibernéticos. A realização do Risk Assessment e a elaboração do Plano Estratégico permitirão:

- Identificar vulnerabilidades e ameaças que possam comprometer a confidencialidade, integridade e disponibilidade dos ativos de informação.
- Priorizar investimentos em segurança com base em riscos reais.
- Estabelecer um roadmap de implementação de controles alinhado às melhores práticas internacionais.
- Fortalecer a postura de segurança de forma sistemática e mensurável.

4.4.3 RISK ASSESSMENT (Análise de Riscos e Controles Cibernéticos)

- A empresa CONTRATADA deverá fornecer entregáveis abrangentes e estruturados que materializarão o trabalho realizado, servindo como referência para a implementação das iniciativas de segurança da informação.
- Estes entregáveis deverão ser elaborados com rigor técnico e clareza comunicativa, equilibrando profundidade analítica com acessibilidade para diferentes públicos dentro da organização. Cada documento deverá ser desenvolvido de forma modular e interconectada, permitindo tanto a consulta independente quanto a compreensão do panorama completo de segurança da informação.
- Os entregáveis deverão ser apresentados em formatos digitais editáveis e em versões finais aprovadas, facilitando atualizações futuras e a integração com outros documentos organizacionais.

4.4.3.1 Análise de riscos e controles cibernéticos

4.4.3.1.1 A CONTRATADA deverá entregar um Relatório de Análise de Riscos e Controles Cibernéticos que apresente uma análise detalhada e sistemática dos riscos de segurança da informação e cibersegurança da organização, servindo como base factual para as decisões estratégicas subsequentes. Essa análise deverá seguir a seguinte dinâmica:

- Levantamento do ambiente

- Mapeamento da infraestrutura de TI (servidores, redes, aplicações críticas);
- Levantamento de políticas, normas e procedimentos de segurança,
- Identificação de requisitos regulatórios aplicáveis.

- Avaliação de controles
  - Análise da efetividade dos controles existentes utilizando como referencias os frameworks NIST CSF 2.0, CIS Controls versão 8.1 e a norma ABNT/IEC ISO 27001;
  - Avaliação de maturidade por domínio de segurança de informação;
  - Análise de controles compensatórios.
- Análise e tratamento de riscos
  - Cálculo de níveis de risco (impacto x probabilidade);
  - Elaboração de matriz de riscos cibernéticos;
  - Definição de estratégias de tratamento (mitigar, transferir, aceitar, evitar);
  - Priorização de riscos para tratamento.

4.4.3.1.2 O documento deverá iniciar-se com um sumário executivo que sintetize os principais achados, tendências identificadas e recomendações prioritárias, proporcionando aos executivos uma visão clara e concisa da postura de segurança atual. O corpo principal do relatório deverá detalhar a metodologia aplicada, o escopo da avaliação e os critérios utilizados para classificação de riscos, estabelecendo a fundamentação técnica que sustenta as conclusões apresentadas.

4.4.3.1.3 A análise de gaps deverá comparar sistematicamente os controles existentes com os requisitos dos frameworks de referência identificando lacunas específicas e oportunidades de melhoria. A avaliação de maturidade por domínio deverá fornecer uma visão granular do nível atual de cada área de segurança, estabelecendo uma linha de base para mensuração de progresso futuro. O relatório deverá concluir com recomendações detalhadas para tratamento dos

riscos identificados, priorizadas segundo critérios de criticidade e viabilidade, e complementadas por apêndices técnicos que documentem evidências e análises detalhadas.

4.4.3.2 Elaboração de plano estratégico de cibersegurança

4.4.3.2.1 A CONTRATADA deverá desenvolver um Plano Estratégico de Cibersegurança que traduza os achados do Relatório de Análise de Riscos e Controles Cibernéticos em um roteiro acionável para evolução da postura de segurança da organização, alinhando iniciativas técnicas com objetivos de negócio.

4.4.3.2.2 O documento deverá estabelecer inicialmente a visão estratégica e os objetivos de segurança para os próximos três anos, articulando claramente como a segurança da informação contribuirá para o sucesso organizacional e definindo metas mensuráveis de maturidade a serem alcançadas.

4.4.3.2.3 O roadmap detalhado de implementação deverá organizar cronologicamente as iniciativas recomendadas, estabelecendo marcos, dependências e responsabilidades para cada ação, e segmentando-as em horizontes de curto, médio e longo prazo.

4.4.3.2.4 O catálogo de iniciativas deverá aprofundar cada ação recomendada, detalhando objetivos específicos, benefícios esperados, recursos necessários, riscos mitigados e interdependências com outras iniciativas.

4.4.3.3 Apresentações

4.4.3.3.1 A CONTRATADA deverá preparar apresentações que complementem os documentos técnicos, traduzindo informações complexas em formatos visuais e narrativos adaptados a diferentes audiências dentro da organização. A apresentação executiva para alta direção deverá sintetizar os principais achados da Análise de Riscos e Controles Cibernéticos e as recomendações estratégicas, utilizando linguagem orientada a negócios e enfatizando implicações financeiras, regulatórias e reputacionais. Esta apresentação deverá ser estruturada para facilitar decisões executivas sobre

investimentos e prioridades, conectando claramente riscos de segurança a objetivos organizacionais.

4.5 TESTE DE INVASÃO

A CONTRATADA deverá realizar, no início da execução do serviço, a Análise de Superfície baseada em MITRE ATT&CK no ambiente tecnológico da CONTRATANTE para reduzir o risco iminente de incidentes de segurança. O assessment de MITRE ATT&CK identifica as técnicas que os adversários podem usar durante um ataque, bem como conceitos e informações básicas sobre grupos de adversários, para avaliar a postura de segurança dos negócios e dos fornecedores de segurança, nesse processo deverão ser checadas a principais táticas de ataque, técnicas e subtécnicas;

Para melhor compreensão deste tópico, devem ser consideradas as seguintes definições:

- Os termos “Pentest”, "teste de penetração", "teste de intrusão" e "teste de invasão", são considerados sinônimos;
- O pentest externo é o tipo de pentest realizado em qualquer dos serviços e sistemas de TI publicados na internet em qualquer porta lógica e que pertençam ao domínio e faixas de IP da CONTRATANTE;
- O pentest interno é o tipo de pentest realizado em serviços e sistemas publicados na intranet (rede interna) da CONTRATANTE, podendo ser concedido acesso remoto à CONTRATADA por meio de VPN, à critério do CONTRATANTE;
- Pentest Black-box: Quando o executor do teste não possui informações acerca do ambiente tecnológico e arquitetura do alvo;
- Pentest Gray-box: Quando o executor do teste tem conhecimento limitado ou algumas informações acerca do ambiente tecnológico e arquitetura do alvo;
- Pentest White-box: Quando o executor tem pleno conhecimento e vasta informação acerca do ambiente tecnológico e arquitetura do alvo.

4.5.1 Os testes de invasão serão realizados semestralmente, sendo seu produto final um relatório detalhado da atividade;

4.5.2 Os testes e avaliações não poderão impactar o pleno funcionamento dos recursos testados, nem ativo porventura relacionado, sem explícita e prévia

autorização e monitoração pela equipe técnica responsável da CONTRATANTE;

4.5.3 Caso a CONTRATANTE entenda haver algum risco na execução do Pentest que possa comprometer, em qualquer grau, o funcionamento de sistema, ativo ou processo da CONTRATANTE, poderá solicitar a mudança de metodologia e/ou do cronograma, inclusive podendo requerer a execução dos testes em finais de semana, feriados ou fora do horário comercial;

4.5.4 A CONTRATADA deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante qualquer das fases de realização do Pentest;

4.5.5 Os sistemas, serviços e ativos de TI da CONTRATANTE a serem submetidos aos testes, serão definidos em Ordens de Serviços (O.S.).

4.5.5.1 A O.S. será elaborada por setor competente do CONTRATANTE, que ficará responsável pelo acompanhamento da execução do teste junto à CONTRATADA.

4.5.5.2 Nas O.S. deverão ser contemplados, no mínimo, os seguintes tópicos (escopo):

4.5.5.2.1 O sistema ou ativo de tecnologia a ser testado;

4.5.5.2.2 A modalidade de pentest a ser realizado (Black Box, Grey Box, White Box).

4.5.5.2.3 Tipo de realização do pentest (Interno ou Externo).

4.5.6 Todos os testes deverão ser acompanhados e supervisionados por setor competente e a critério do CONTRATANTE;

4.5.7 Durante os testes, não poderão ser executados quaisquer variações dos seguintes ataques sem explícita autorização prévia e monitoração pela equipe técnica responsável da CONTRATANTE:

4.5.7.1 Ataques de negação de serviços e flooding;

4.5.7.2 Engenharia social, por exemplo, phishing, vishing, pharming, personificação, roubo de identidade e outros;

4.5.7.3 Ataques que possam causar danos físicos, por exemplo, arrombamentos, danos às fechaduras eletrônicas, ativação de sistemas de alarme;

4.5.7.4 Ataques que envolvam vetores de infecção, tais como, ransomware, vírus, worms, trojan, rootkits e outros.

4.5.8 A CONTRATADA deve elaborar junto com a CONTRATANTE o plano de ação para correção das falhas.

4.5.9 Cada teste de intrusão, necessariamente, deverá seguir as seguintes fases, nesta ordem:

4.5.9.1 PLANEJAMENTO - A partir de Ordem de Serviço (OS) requisitada pela CONTRATANTE inicia-se a fase de Planejamento, quando serão apresentados e discutidos os itens constantes na OS;

4.5.9.1.1 Na fase de planejamento serão definidos:

4.5.9.1.2 Pacote de invasão/Pentest ou a quantidade de horas a serem consumidas;

4.5.9.1.3 Objetivo de “comprometer o ambiente” para ser alcançado como por exemplo. Caso o objetivo mude durante a tentativa, deve ser reportado em relatório posterior;

4.5.9.1.4 Processos e atividades permitidas ou proibidas;

4.5.9.1.5 O detalhamento do cronograma;

4.5.9.1.6 As informações e acessos necessários para a realização do Pentest (especialmente nos casos de Pentests Graybox e Whitebox);

4.5.9.1.7 A fase de Planejamento será formalizada através de declaração de aceite contendo todas as informações discutidas e definidas.

4.5.9.2 DESCOBERTA - Após formalmente autorizado pela CONTRATANTE, inicia-se a fase de Descoberta, que tem como objetivo a obtenção de informações relevantes dentro do escopo do teste que possibilitam reconhecer possíveis ameaças/vulnerabilidades. Importante frisar que esta fase não deve se restringir à utilização de ferramentas automatizadas, sendo esperada atuação manual da equipe técnica contratada, aprofundando a análise da superfície de ataque à procura de vulnerabilidades não facilmente identificáveis. Deverão ser realizadas, no mínimo, as seguintes atividades:

4.5.9.2.1 Coleta passiva, caracterizada pela obtenção de informações utilizando-se, no mínimo, as seguintes técnicas/serviços/ferramentas, quando aplicáveis:

4.5.9.2.1.1 Whois e nslookup (consultas DNS);

4.5.9.2.1.2 Sites de busca;

4.5.9.2.1.3 Listas de discussão;

4.5.9.2.1.4 Blogs de colaboradores;

4.5.9.2.1.5 Dumpster diving ou trashing;

4.5.9.2.1.6 Informações livres;

4.5.9.2.1.7 Packet sniffing “passive eavesdropping”;

4.5.9.2.1.8 Captura de banner.

4.5.9.2.2 Coleta ativa, onde deverá ser utilizada, no mínimo, as seguintes técnicas, quando aplicáveis:

4.5.9.2.2.1 Port scanning (Mapeamento de rede);

4.5.9.2.2.2 Varredura de vulnerabilidade.

4.5.9.3 EXPLORAÇÃO - Nesta fase, o objetivo é confirmar as vulnerabilidades e identificar os impactos e riscos das ameaças porventura encontradas a partir de simulações de ataques reais. As ações desta fase devem utilizar metodologias reconhecidas no mercado e elencadas neste estudo e não devem comprometer o correto funcionamento dos equipamentos e sistemas, nem afetar o desempenho das atividades ora realizadas na CONTRATANTE, exceto sob prévia e expressa autorização e monitoração pela equipe técnica responsável dela. Além disso, deve-se atender os seguintes itens:

4.5.9.3.1 A empresa CONTRATADA deverá ser capaz de aplicar, no mínimo, os seguintes tipos de ataques, quando aplicáveis:

4.5.9.3.1.1 Violações do protocolo HTTP;

4.5.9.3.1.2 SQL Injection;

4.5.9.3.1.3 LDAP Injection;

4.5.9.3.1.4 Cookie Tampering;

4.5.9.3.1.5 Cross-Site Scripting (XSS);

4.5.9.3.1.6 Directory Transversal;

4.5.9.3.1.7 Buffer Overflow;

4.5.9.3.1.8 OS Command Execution;

4.5.9.3.1.9 Command Injection;

4.5.9.3.1.10 Remote Code Inclusion;

4.5.9.3.1.11 Server Side Includes (SSI) Injection;

4.5.9.3.1.12 File disclosure;

4.5.9.3.1.13 Information Leak;

4.5.9.3.1.14 Problemas com o SNMP.

4.5.9.3.2 Para testes de invasão direcionados, especialmente, aos serviços prestados via WEB, tanto Intranet quanto Internet, deverão ser observados e aplicados, no mínimo, os testes baseados na publicação OWASP TESTING GUIDE (The Open Web Application Security Project) em sua versão mais recente;

4.5.9.3.3 Qualquer vulnerabilidade crítica e de fácil exploração encontrada deverá ser imediatamente comunicada à equipe técnica da CONTRATANTE, contendo detalhes técnicos e ações necessárias para a correção da vulnerabilidade e disponibilizado de forma segura em até 1 (um) dia útil. Caso ocorra antes do término do teste, deverá ser reportado no relatório se houve impacto na continuidade do teste.

4.5.9.4 RELATÓRIO - Após a fase de Exploração, deve ser elaborado pela CONTRATADA um relatório do teste de intrusão. Este relatório deve conter ao menos:

4.5.9.4.1 Escopo, tipo e modalidade do teste;

4.5.9.4.2 Metodologias, técnicas, fontes de pesquisa, referências, equipamentos e ferramentas utilizadas;

4.5.9.4.3 Atividades realizadas, em ordem cronológica;

4.5.9.4.4 Tempo do analista utilizado em cada atividade;

4.5.9.4.5 Informações acessadas e detalhes da infraestrutura descoberta, caso aplicável;

4.5.9.4.6 Confirmação ou refutação de existência das vulnerabilidades;

4.5.9.4.7 Descrição de todas as vulnerabilidades e ameaças porventura encontradas, informando, no mínimo:

4.5.9.4.7.1 Nome;

4.5.9.4.7.2 Nível de Risco;

4.5.9.4.7.3 Intrusiva (sim / não);

4.5.9.4.7.4 Descrição;

4.5.9.4.7.5 Observação;

4.5.9.4.7.6 Recomendação de Remediação;

4.5.9.4.7.7 Link do patch ou da correção;

4.5.9.4.7.8 Número CVE, se houver;

4.5.9.4.7.9 SANS / FBI referência Top 20;

4.5.9.4.7.10 IAVA (Information Assurance Vulnerability Alert) Referência.

4.5.9.4.7.11 Detalhamento do caminho utilizado e evidências da exploração das vulnerabilidades porventura encontradas.

4.5.9.4.7.12 Tipos de ataques realizados;

4.5.9.4.7.13 Avaliação de riscos e impacto da vulnerabilidade e consequente exploração;

4.5.9.4.7.14 Contramedidas para correção ou mitigação dos riscos decorrentes das vulnerabilidades encontradas;

4.5.9.4.7.15 Anexos com os resultados dos testes automatizados e vídeos de realização dos ataques bem-sucedidos, quando assim solicitados;

4.5.9.4.7.16 Prover informações sobre a efetividade da simulação, apresentando ao menos:

4.5.9.4.7.16.1 Quantidade de usuários testados;

4.5.9.4.7.16.2 Quantidade de usuários que somente visualizaram;

4.5.9.4.7.16.3 Quantidade de usuários que clicaram em algum link/anexo;

4.5.9.4.7.16.4 Quantidade de usuários enganados;

4.5.9.4.7.16.5 Tempo decorrido desde a última simulação;

4.5.9.4.7.16.6 Deve estar disponível, pelo menos, em português e inglês;

4.5.9.4.7.16.7 Alerta de Vulnerabilidades.

4.5.9.4.8 A CONTRATADA deverá elaborar e coordenar um plano de ação para a correção das vulnerabilidades encontradas;

4.5.9.4.9 A CONTRATADA deverá abrir chamados no sistema de atendimento da CONTRATANTE de modo a solicitar às áreas pertinentes a correção das vulnerabilidades identificadas;

4.5.9.4.10 Tais chamados devem ser abertos por ação corretiva, agrupando todas as vulnerabilidades eliminadas pela execução daquela ação.

4.5.9.4.11 A CONTRATADA deverá acompanhar a resolução dos chamados abertos, validando as evidências e dando baixa nas vulnerabilidades tratadas no sistema de gestão de vulnerabilidades.

4.6 DETECÇÃO E RESPOSTA A INCIDENTES

4.6.1 A CONTRATADA deverá disponibilizar solução completa de Detecção e Resposta a Incidentes de Segurança, com desempenho e capacidade adequada para atender a execução do serviço proposto;

4.6.2 Monitoração e detecção de ameaças

4.6.2.1 Gestão de incidentes com foco na priorização e escalonamento, baseado de riscos cibernéticos e impactos a organização;

4.6.2.2 O ambiente a ser monitorado possui até 23.552 (vinte e três mil quinhentos e cinquenta e dois) ativos, incluindo servidores, estações de trabalho, roteadores, switchs, entre outros;

4.6.2.2.1 A solução deverá estar licenciada, operacional e funcional de forma a abranger toda a infraestrutura de TIC da CONTRATANTE;

4.6.2.2.2 Durante toda a vigência do contrato, não deve existir para a solução ofertada limitação quanto a quantidade de consultas de usuário nem de consultas programáticas (queries) às informações, quantidade de parses no tratamento de eventos, quantidade de conectores para ingestão, quantidade de envio de registros por ativo, quantidade de casos de uso.

4.6.2.3 Detectar, escalonar, notificar e recomendar boas práticas para redução do risco cibernético de acordo com o plano de resposta a incidentes. A monitoração deve ser centralização em solução de gestão de segurança da CONTRATADA, próximo ao tempo real;

4.6.2.4 A CONTRATADA deverá integrar-se com as diversas soluções existentes e em uso pela CONTRATANTE, bem como intervir, em caso de resposta a incidentes críticos, tais como:

- Solução de antivírus EDR/XDR
- Solução de correio eletrônico
- Solução de domínio de rede (Active Directory/Novell/Open LDAP) e domínios de nomes (Bind/DNS)
- Solução de virtualização

- Solução de proxy de saída (squid proxy e filtro de conteúdo)
- Solução de firewall de borda interna/externa e suas camadas de proteção: antivírus, ips, ids, anti-bot, anti-spam, anti-ddos, anti-phishing, anti-malware, url filters.
- Solução de microssegmentação de tráfego de rede
- Solução de balanceamento de carga e WAF (ASM, AFM, LTM e DataIQ)
- Dispositivos de rede, concentradores de rede (roteador, switches de bordas etc.).

4.6.2.5 Monitoramento de vazamento de dados e proteção dos sistemas gerenciadores de banco de dados;

4.6.2.6 Detectar, analisar, elaborar relatórios de riscos e escalonar entre os níveis de perfil de profissionais, para que sejam tratados de acordo com a severidade do evento ou incidente de segurança

4.6.2.7 Caberá ao gerente, a avaliação do incidente e notificar em até 20 minutos, de acordo com o plano de comunicação, sobre a ocorrência da ameaça identificada, quando houver alto risco de segurança ao ambiente de TI da CONTRATANTE;

4.6.2.8 Deverá ser realizado acompanhamento periódico dos indicadores de segurança, para que formulação de planos de ação para mitigação de falhas de segurança;

4.6.2.9 Para resposta ao incidente de segurança, a equipe de SOC deverá atuar de forma preventiva com orquestração e automação de “playbooks” que atuem diretamente nas soluções existentes da CONTRATADA;

4.6.2.10 Disponibilizar rastreio de acesso e logs de ações e atuações no ambiente da CONTRATANTE para fins de auditoria;

4.6.2.11 Preservar, coletar e manter as evidências dos incidentes, para fins de investigação e documentação do evento de segurança;

4.6.2.12 Detectar, Identificar e corrigir incidentes documentados e registrar na ferramenta de ITSM da CONTRATADA

4.6.2.13 Os incidentes não documentos, devem ser escalonados para os demais níveis de perfil de profissional para que sejam investigados, tratado e documentos na base de conhecimento.

4.6.2.14 Geração de relatórios, dashboards e perfis de acesso conforme a relevância dos eventos;

4.6.2.15 Atuar na prevenção de ameaças, aplicando boas práticas de segurança que minimizem os riscos de segurança.

4.6.3 Resposta a incidentes e cenários de crise

4.6.3.1 A CONTRATADA deverá possuir um conjunto de processos, procedimentos e práticas utilizadas para lidar com incidentes de segurança da informação em uma organização. Esses incidentes podem variar desde ataques cibernéticos (como malware, ransomware ou phishing) até falhas de segurança que expõem dados sensíveis ou interrupções no serviço com objetivo de minimizar o impacto dos incidentes, conter os danos, restaurar os sistemas afetados e evitar que o incidente ocorra novamente;

4.6.3.2 A CONTRATADA deverá possuir um processo de resposta a incidentes estruturada em etapas que formam um ciclo contínuo de melhoria. As etapas devem seguir o Ciclo de Resposta a Incidentes de acordo com o framework NIST (National Institute of Standards and Technology) ou o SANS Institute;

4.6.3.3 A CONTRATADA deverá gerar um relatório técnico e executivo ao final de cada Resposta a Incidente para evidenciar as fases de Preparação, Identificação, Contestação, Erradicação, Recuperação e Lições Aprendidas;

4.6.3.4 Deverá atuar conforme o plano de resposta a incidentes, que deve ser atualizado mensalmente, para os acionamentos dos papeis e responsabilidades de acordo com ocorrência do evento de crise;

4.6.3.5 Em eventual cenário de crise, em que ocorra um ataque cibernético ou um problema de segurança crítico que possa afetar a disponibilidade, a CONTRATADA deverá disponibilizar uma sala virtual de crise, para reuniões emergências para tratamento da crise

4.6.3.6 A contratada deverá disponibilizar equipe técnica para deslocamento até o local do Datacenter da contratante para mitigar o incidente de segurança, em conjunto com a equipe técnica da contratante.

4.6.3.7 O evento de crise, poderá ocorrer, em qualquer horário e dia, inclusive finais de semana, feriados e pontos facultativos

4.6.3.8 Não haverá ônus a contratante para despesas de deslocamento, alimentação ou quaisquer outros gastos que venham a ocorrer.

4.6.3.9 A solução ofertada deve contemplar, de forma integrada e nativa, minimamente os seguintes mecanismos de detecção de incidentes

4.6.3.9.1 Correlacionamento de eventos (SIEM);

4.6.3.9.2 Análise comportamental de usuários (UEBA);

4.6.3.9.3 Detecção de intrusão (IDS);

4.6.3.9.4 Malware Sandbox;

4.6.3.10 A solução ofertada deve permitir o Gerenciamento, análise, orquestração e automação de políticas, posturas, casos de uso, playbooks e integrações, com capacidade de resposta autônoma e aplicação próxima a tempo real, com componente de Orquestração, Automação e Resposta de Segurança (SOAR), totalmente e nativamente integrado à solução, com o objetivo de automatizar os processos e fluxos de trabalho, a execução de atividades repetitivas ou de difícil execução e a orquestração das diversas ferramentas de segurança, sem necessidade de atuação humana;

4.6.3.11 Para tal, a CONTRATADA deverá fazer uso de uma plataforma unificada para Detecção e Resposta Estendida com as seguintes características e especificações:

4.6.3.11.1 Quanto ao armazenamento de logs e eventos, a solução ofertada deverá:

4.6.3.11.1.1 Armazenar, na própria solução, as informações do tráfego de rede e dos Logs durante o período, mínimo, de 30 dias ininterruptos, bem como o registro dos incidentes gerados pela plataforma durante o período de 365 dias ininterruptos;

4.6.3.11.1.2 Permitir a retenção do histórico de segurança da CONTRATADA, contemplando, minimamente, os seguintes dados:

i. Dados de eventos de segurança;

ii. Dados das aplicações;

iii. Dados dos sistemas operacionais;

iv. Dados das nuvens públicas e privadas;

v. Dados do tráfego de rede;

vi. Tráfego de registro (syslog).

4.6.3.11.2 Quanto à compatibilidade e integrações, a solução ofertada deverá:

4.6.3.11.2.1 Ser capaz de integrar-se às soluções de segurança terceiras presentes na rede, a fim de enriquecer a análise das informações coletadas e permitir ações adicionais de bloqueio contra-ataques cibernéticos;

4.6.3.11.2.2 Possuir uma API restful para integração com vários serviços para ingestão de logs, telemetria e tráfego para detecção e resposta a eventos de segurança;

4.6.3.11.2.3 Ser compatível com plataformas Windows e Linux;

4.6.3.11.2.4 Permitir a inspeção de plataformas como:

- Amazon AWS;
- Microsoft Azure;
- Google G-Suite;
- Microsoft Office 365;
- Componentes virtuais (máquinas virtuais);
- Box.

4.6.3.11.3 Quanto ao mecanismo de gerenciamento e correlação de eventos (SIEM), a solução ofertada deverá:

4.6.3.11.3.1 Possuir a capacidade de realizar a coleta e a ingestão de logs de todos os componentes do ambiente tecnológico da CONTRATANTE, através do padrão syslog ou similar;

4.6.3.11.3.2 Correlacionar eventos, com o objetivo de identificar anomalias e incidentes automaticamente.

4.6.3.11.4 Quanto a detecção dos incidentes, a solução ofertada deverá:

4.6.3.11.4.1 **S**er capaz de detectar padrões de ataques sem a utilização de assinaturas, através da elaboração automatizada de um baseline comportamental dos usuários e entidades;

4.6.3.11.4.2 Possuir a capacidade de, via técnicas de Machine Learning, identificar anomalias nos comportamentos individuais dos usuários e entidades e de gerar alertas com relação, ao menos, aos seguintes casos de uso:

- Horário atípico do acesso;

- Número atípico de sessões de uso nos sistemas operacionais;
- Volume de conexões atípico;
- Volume de transferências de dados atípico;
- Localização geográfica atípica da origem do acesso;
- Endereço IP de origem atípico do acesso;
- Acesso atípico a dados armazenados;
- Criação e uso de processos (executáveis em memória) atípicos pelo usuário/entidade;
- Mudança na postura de risco do usuário/entidade.

4.6.3.11.4.3 Possuir mais de 150 modelos de detecção para casos de uso, como, no mínimo, Ransomware, Command & Control, DGA, Cryptojacking, phishing, scripts de Powershell maliciosos, UBA e ataques de zero-day;

4.6.3.11.4.4 Permitir a criação de novas regras de detecção e alteração das regras existentes;

4.6.3.11.4.5 Emitir alertas quando eventos críticos de segurança forem detectados na rede e estes se desviarem de padrões estabelecidos (anomalias), por meio de análises detalhada de cada aplicativo em execução na rede de modo nativo, gerando chamados para a equipe do SOC, automaticamente, para a sua atenção, atuação e documentação;

4.6.3.11.4.6 Permitir a geração de diagramas de conexões TCP mostrando como as ameaças estão associadas, bem como se movem no ambiente, baseado em capturas de tráfego, classificados e normalizadas automaticamente.

4.6.3.11.5 Quanto a resposta aos incidentes, a solução ofertada deverá:

4.6.3.11.5.1 Incluir uma solução integrada de gerenciamento de casos e incidentes;

4.6.3.11.5.2 Ter a capacidade de associar vários alertas recebidos a um único incidente que tem a capacidade de ser atribuído, ter uma linha do tempo, objetos associados, bem como as principais métricas MTTD e MTTR;

4.6.3.11.5.3 Ter a capacidade de enviar instruções de resposta através dos mesmos sensores de coleta;

4.6.3.11.5.4 Ter a capacidade de responder a todos os eventos de forma orquestrada e automatizada, integrando-se ao ambiente tecnológico da CONTRATANTE. As ações possíveis de resposta devem ser, pelo menos, as seguintes:

- Enviar um e-mail;
- Enviar mensagens para meios de comunicação do tipo SLACK;
- Fazer um POST, GET ou um PUT para um servidor;
- Criar regras de bloqueio no firewall;
- Desabilitar usuários no Active Directory;
- Executar scripts.

4.6.3.11.5.5 Contemplar uma ferramenta que permita a investigação e busca de ameaças, com o objetivo de identificar as ameaças presentes na rede e automatizar os eventos de segurança para responder a elas;

4.6.3.11.5.6 Ser capaz de realizar análise retrospectiva com base nos dados ingeridos e armazenados do tráfego TCP/UDP, apoiando uma análise forense.

4.6.3.11.6 Quanto aos relatórios e dashboards, a solução ofertada deverá:

4.6.3.11.6.1 Ter a capacidade de gerar relatórios executivo e operacionais, com base em modelos pré-configurados, personalizáveis, baseados em dashboards, incluindo, pelo menos, relatórios sobre o status atual dos dispositivos, seu risco associado e tendências;

4.6.3.11.6.2 Gerar informações detalhadas sobre os eventos detectados, incluindo ameaças, anomalias, comportamentos e tendências de rede associadas ao risco de rede;

4.6.3.11.6.3 Detalhar os gráficos para aprofundar as informações apresentadas (mecanismo conhecido como Drill Down);

4.6.3.11.6.4 Gerar KRI (Principais Indicadores de Risco), como o número de eventos gerados em um dia, semana ou meses e compará-los com um período semelhante, o mesmo com a criticidade média dos eventos;

4.6.3.11.6.5 Permitir ao pessoal designado a geração de relatórios explorando todas as variáveis e funcionalidades da ferramenta, com a opção de parametrizar esses relatórios e consultá-los via Web, bem como a criação de filtros personalizados para pesquisas de eventos específicos;

4.6.3.11.6.6 Fornecer painéis configuráveis que possam conter diferentes gráficos com informações de, pelo menos:

- *Eventos anômalos e críticos, incluindo:*
- *Detecções de segurança;*
- *IPs de Origem e Destino;*
- *Visão geral da atividade dos dispositivos (servidores e infraestrutura, física e virtualizada);*
- *Táticas e técnicas do MITRE ATT&CK;*
- *Fases do Kill Chain e os alertas associados.*
- *Aplicações utilizadas e seus dados históricos, discriminada por:*
    - *Risco associado;*
    - *IP de Origem e Destino;*
    - *Anomalias detectadas;*
    - *Classificação de risco;*
    - *Tráfego entre hosts.*
    - *Informações de em um Host:*
    - *Aplicações utilizadas;*
    - *Tráfego de e para o Host com base em detecções de segurança e anomalias.*
- *Informações e o status das aplicações e serviços que estão sendo executados no data center, tais como:*
- *Quantidade e a gravidade das anomalias;*
- *Possíveis problemas de segurança no data center.*

4.6.3.11.6.7 Permitir a criação de relatórios por período (hora, dia, semana, mês, ano, e personalizado por datas específicas);

4.6.3.11.6.8 Possuir filtros pós-captura, pelo menos para:

- *Filtro de erro;*

- *Filtros por tráfego entre duas estações através da seleção do nome ou endereço IP;*
- *Filtros por protocolos;*
- *Geolocalização;*
- *Gravidade;*
- *Endereço IP.*

4.6.3.11.6.9 Suportar diagnósticos nas diferentes camadas do modelo OSI, incluindo:

- *Análise das anomalias da rede da camada 2 à camada 7;*
- *Endereços IP;*
- *Aplicações e/ou portas (TCP/UDP);*
- *Serviços associados;*
- *Servidores mais lentos;*
- *Origem e destino.*

4.6.3.11.6.10 Ser capaz de gerar um gráfico das anomalias das aplicações dentro da rede, fornecendo resultados com pelo menos as seguintes variáveis:

- *Movimentos laterais;*
- *Histórico de eventos;*
- *Anomalias de tráfego maliciosos;*
- *Anomalias de políticas e negações de firewalls de infraestrutura;*
- *Principais Aplicações;*
- *Top Servidores;*
- *Top Clientes;*
- *Status das sessões atuais;*
- *Origens e destinos de países com má reputação.*

4.6.3.11.6.11 Exportar as informações dos pacotes capturados em metadados para análise posterior.

4.6.4 Análise de causa raiz

4.6.4.1 Para cada incidente identificado deverá ser elaborado e entregue um relatório detalhando minimamente:

4.6.4.1.1 Os impactos observados;

4.6.4.1.2 A(s) vulnerabilidade(s) explorada(s);

4.6.4.1.3 O método de ataque;

4.6.4.1.4 A origem do ataque.

4.7 CIBERVIGILÂNCIA

Para melhor compreensão deste tópico, devem ser consideradas as seguintes definições:

- Proteção Proativa: Identifica e mitiga ameaças antes que se materializem em ataques.
- Visibilidade Ampliada: Oferece uma visão abrangente do perfil de risco digital da organização.
- Conformidade Regulatória: Auxilia no cumprimento de normas de segurança e privacidade de dados.
- Economia de Recursos: Automatiza processos de monitoramento, reduzindo a carga sobre equipes internas.
- Inteligência Acionável: Fornece insights valiosos para tomada de decisões estratégicas de segurança.

4.7.1 Requisitos gerais

4.7.1.1 A solução de Cibervigilância se aplica ao domínio prefeitura.rio e todos os seus subdomínios, bem como a 50 usuários VIP;

4.7.1.2 Solução ofertada em modo SAAS, sem a necessidade de instalação de componentes no ambiente da CONTRATANTE ou nos ambientes monitorados;

4.7.1.3 Licenciamento por domínio principal, sem cobrança adicional por subdomínios, quantidade de endereços IP e quantidade de usuários;

4.7.1.4 Funcionalidades EASM (External Attack Surface Management), DRPS (Digital Risk Protection Services), SRS (Scoring Risk Services), BRM (Branding Monitoring e TPRA (Third Parties Risk Management) integradas;

4.7.1.5 Solução de cibervigilância e ciberinteligência, com recursos de inteligência artificial e automação, permitindo uma detecção mais rápida e precisa de ameaças em tempo real sem necessidade de intervenção humana;

4.7.1.6 Mapeamento dinâmico do perímetro de ataque digital, monitoramento e detecção automática de informações expostas, através de robôs de busca automatizados;

4.7.1.7 Análise não intrusiva e monitoramento contínuo 24/7;

4.7.1.8 Monitoramento abrangente para uma visão mais completa dos riscos cibernéticos, através da obtenção de dados de diversas fontes, tais como Internet superficial, Deep Web, Dark Web e Redes sociais;

4.7.1.9 A solução deve aprender e obter informações de forma autônoma, sem a necessidade de fornecimento de informações como palavras-chave, ativos, fontes, datas ou outros dados específicos;

4.7.1.10 A curva de aprendizado da ferramenta deve ser simples e não exigir informações ou configurações específicas;

4.7.1.11 A solução deve possuir uma metodologia específica para controle de falsos positivos, estabelecendo contextos de busca configuráveis pelo usuário;

4.7.1.12 Avaliação de riscos e pontuação de segurança cibernética em tempo real;

4.7.1.13 Identificação proativa de riscos;

4.7.1.14 Análise de riscos de terceiros e fornecedores;

4.7.1.15 A solução deverá dispor de equipe especializada em inteligência e ameaças cibernéticas para geração de novos contextos, gerenciamento de remoção de conteúdo, criação de regras, revisão, aprovação, automação e melhoria contínua da plataforma.

4.7.2 Interface do usuário

4.7.2.1 Deve fornecer uma avaliação geral de risco o mais próximo possível do aparecimento da ameaça;

4.7.2.2 Deve fornecer uma descrição e recomendação de correção para cada vulnerabilidade;

4.7.2.3 Deve exibir graficamente cada vulnerabilidade identificada por gravidade;

4.7.2.4 Exibição gráfica para cada vulnerabilidade identificada;

4.7.2.5 Deve rastrear o histórico e exibir graficamente categorias associadas à análise de vulnerabilidade externa;

4.7.2.6 Exibir uma lista com as três principais vulnerabilidades graves.

4.7.3 Monitoramento de dados de usuários VIP:

4.7.3.1 Licenciamento baseado no número de usuários VIP monitorados;

4.7.3.2 Capacidade de monitorar dados pessoais sensíveis de usuários VIP, tais como documentos de identificação, informações bancárias, cartões de crédito e Wallets Bitcoin, mediante autorização e entrada dessas informações pelo próprio usuário VIP na plataforma;

4.7.3.3 Os dados pessoais sensíveis dos usuários VIP devem ser protegidos por criptografia, mascaramento e controle de acesso, impedindo que qualquer pessoa além do proprietário dos dados, mesmo os administradores da plataforma, venham a ter acesso a esses dados;

4.7.3.4 Monitoramento contínuo das informações pessoais quanto à vazamento de informações ou atividades suspeitas que possam representar ameaça à integridade pessoal ou patrimonial da pessoa protegida;

4.7.3.5 Capacidade de análise de postagens e interações em redes sociais que possam ameaçar a integridade da pessoa protegida.

4.7.4 Monitoramento e Análise Avançados

4.7.4.1 Monitoramento contínuo 24/7/365 da Internet superficial, Deep Web e Dark Web;

4.7.4.2 Análise de redes sociais, fóruns, marketplaces ilegais e canais de mensagens;

4.7.4.3 Capacidade de monitorar pelo menos 100 milhões de fontes de dados diferentes;

4.7.4.4 Monitoramento não intrusivo, totalmente autônomo e automatizado, sem a necessidade de intervenção humana;

4.7.4.5 Identificação automática de vazamentos de dados, credenciais comprometidas e informações sensíveis expostas;

4.7.4.6 Detecção de menções à marca, executivos e ativos digitais da organização em contextos maliciosos;

4.7.4.7 Alertas em tempo real para ameaças emergentes, com priorização baseada em gravidade e relevância.

4.7.5 Monitoramento da Superfície de Ataque

4.7.5.1 Descoberta e inventário automático de ativos digitais expostos (domínios, subdomínios, endereços IP, etc);

4.7.5.2 Identificação de vulnerabilidades em sistemas e aplicações expostos à internet;

4.7.5.3 Monitoramento contínuo de alterações na superfície de ataque digital, incluindo:

4.7.5.3.1 Rede: exposição e possível nível de risco representado pela rede da organização;

4.7.5.3.2 Integridade do DNS: Subdomínios públicos e análise de domínios maliciosos ou suspeitos de phishing: Detecção de páginas falsas, para fraude, fraude, phishing ou roubo de dados;

4.7.5.3.3 Vazamento de Dados: Vazamento de dados pessoais ou informações corporativas confidenciais, sensíveis e protegidas;

4.7.5.3.4 Credenciais vazadas: detecção em tempo real de credenciais que representam a possibilidade de acesso privilegiado;

4.7.5.3.5 Análise Web: status de proteção do CMS, patches, plug-ins e suas configurações e atualizações;

4.7.5.3.6 Reputação de IP: Comportamento anômalo dos IPs de domínio, indicativo de elementos infectados;

4.7.5.3.7 Gerenciamento de Patches: Informações obtidas a partir da análise de CVEs em tempo real conforme definido na norma;

4.7.5.3.8 Segurança de Email: Verificação e validação de configuração e detecção de informações ou e-mails vazados;

4.7.5.3.9 Inteligência em Redes Sociais: Detecção de ameaças e riscos através da análise de conversas em redes sociais (Hacktivismo, Fraude, Fake News, Impersonation, discurso de ódio).

4.7.5.4 As fontes de monitoramento devem considerar, no mínimo:

4.7.5.4.1 Internet, Deep Web e Dark Web: A análise da Dark Web não se limitará apenas à conhecida rede Tor. Outras redes que também fazem parte da Dark Web deverão ser incluídas no monitoramento;

4.7.5.4.2 Sites Git: onde os programadores compartilham código, como GitHub e similares;

4.7.5.4.3 “Paste” sites: onde são compartilhados fragmentos de texto que podem ser códigos ou informações não estruturadas, como PasteBin e similares;

4.7.5.4.4 Fóruns: onde os usuários compartilham informações de vários tipos, como Reddit, Breached.vc ou similares;

4.7.5.4.5 Sites de informação: repositórios genéricos de informações compartilhadas, como Discord ou IRC.

4.7.6 Avaliação de Riscos e Inteligência de Ameaças

4.7.6.1 Pontuação de Risco Cibernético

4.7.6.1.1 Cálculo dinâmico de score de risco baseado em múltiplos fatores (exposição, ameaças, vulnerabilidades);

4.7.6.1.2 Benchmarking de risco em relação a pares da indústria e melhores práticas de segurança;

4.7.6.1.3 Recomendações acionáveis para melhoria do perfil de risco.

4.7.6.2 Avaliação de Terceiros

4.7.6.2.1 Monitoramento contínuo de riscos associados a fornecedores, parceiros e clientes;

4.7.6.2.2 Avaliação automatizada de postura de segurança de terceiros;

4.7.6.2.3 Alertas sobre mudanças significativas no perfil de risco de entidades relacionadas;

4.7.6.2.4 Possibilidade de conhecer em detalhe as vulnerabilidades caso desejado.

4.7.6.3 Inteligência de Ameaças Contextualizada

4.7.6.3.1 Coleta e análise de indicadores de comprometimento (IoCs) relevantes para a organização;

4.7.6.3.2 Correlação de dados de ameaças com o ambiente específico da organização;

4.7.6.3.3 Geração de relatórios de inteligência personalizados e acionáveis.

4.7.6.4 Proteção de Dados e Propriedade Intelectual

4.7.6.4.1 Detecção de vazamentos de dados sensíveis, incluindo dados pessoais, dados pessoais sensíveis e dados financeiros;

4.7.6.4.2 Monitoramento de exposição de propriedade intelectual (código-fonte, segredos comerciais, patentes).

4.7.6.5 Gestão de Reputação Digital

4.7.6.5.1 Monitoramento de sentimento e menções à marca em mídias sociais e fóruns online;

4.7.6.5.2 Detecção de campanhas de desinformação ou ataques coordenados à reputação;

4.7.6.5.3 Alertas sobre uso não autorizado de marcas registradas ou propriedade intelectual.

4.7.7 Requisitos Técnicos e de Implementação

4.7.7.1 Tecnologia e Arquitetura

4.7.7.1.1 Inteligência Artificial e Machine Learning

4.7.7.1.1.1 Utilização de modelos de IA para detecção de anomalias e padrões de ameaças;

4.7.7.1.1.2 Algoritmos de aprendizado de máquina para redução de falsos positivos e priorização de alertas;

4.7.7.1.1.3 Capacidade de processamento de linguagem natural para análise de conteúdo em múltiplos idiomas.

4.7.7.1.2 Automação Avançada

4.7.7.1.2.1 Crawlers e scrapers automatizados para coleta contínua de dados da web;

4.7.7.1.2.2 Workflows automatizados para resposta a incidentes e mitigação de riscos.

4.7.7.1.3 Escalabilidade e Desempenho

4.7.7.1.3.1 Arquitetura distribuída capaz de processar e analisar petabytes de dados;

4.7.7.1.3.2 Tempo de alerta inferior a 5 minutos para alertas críticos;

4.7.7.1.3.3 Capacidade de escalar horizontalmente para acomodar crescimento de dados e usuários.

4.7.7.2 Integração e Interoperabilidade

4.7.7.2.1 APIs RESTful documentadas para integração com sistemas de segurança existentes (SIEM, SOAR, etc.);

4.7.7.2.2 APIs para plataformas populares de segurança e gerenciamento de riscos.

4.7.7.3 Segurança e Conformidade

4.7.7.3.1 Proteção de ponta a ponta para todos os dados em trânsito e em repouso;

4.7.7.3.2 Autenticação multifator e controle de acesso baseado em funções (RBAC);

4.7.7.3.3 Conformidade com padrões de segurança (ISO 27001, SOC 2) ou equivalente e regulações de privacidade (GDPR, CCPA).

4.7.7.4 Experiência do Usuário

4.7.7.4.1 Dashboard personalizável com visualizações interativas de dados e riscos;

4.7.7.4.2 Interface responsiva otimizada para desktop e dispositivos móveis;

4.7.7.4.3 Suporte multilíngue.

4.7.8 Capacidades de IA e Automação Essenciais

4.7.8.1 Análise Preditiva de Ameaças

4.7.8.1.1 Utilização de modelos de machine learning para prever tendências de ameaças e ataques potenciais;

4.7.8.1.2 Capacidade de identificar padrões sutis que indicam preparação para ataques cibernéticos.

4.7.8.2 Detecção de Anomalias Baseada em IA

4.7.8.2.1 Algoritmos de aprendizado não supervisionado para identificar comportamentos anômalos em redes e sistemas;

4.7.8.2.2 Adaptação contínua a padrões de tráfego e atividade normais para reduzir falsos positivos.

4.7.8.3 Processamento de Linguagem Natural Avançado

4.7.8.3.1 Análise semântica de conteúdo em múltiplos idiomas para identificar ameaças e intenções maliciosas;

4.7.8.3.2 Capacidade de entender contexto e nuances em comunicações relacionadas a ameaças.

4.7.8.4 Enriquecimento e Correlação de Dados Automatizados

4.7.8.4.1 Agregação e correlação automática de dados de múltiplas fontes para criar inteligência acionável.

4.8 SIMULAÇÃO DE AMEAÇAS

4.8.1 A CONTRATADA deverá disponibilizar solução de simulação de ameaças e análise de postura dos controles de segurança, com o objetivo de simular a

exploração das vulnerabilidades reportadas de modo a priorizá-las e que seja testado a efetividade do plano de remediação proposto;

4.8.1.1 Implantação, planejamento, execução, análise e relatório de testes automatizados, repetíveis e continuados de segurança com ferramenta de simulação de violações e ataques (breach and attack simulation – BAS), visando:

4.8.1.1.1 Avaliar e validar a eficácia operacional dos controles de segurança e identificar as lacunas na cadeia e postura de segurança;

4.8.1.1.2 Avaliar e validar se as fontes de registros e telemetria e as regras de monitoramento, detecção e resposta estão sendo capturadas pela ferramenta de monitoramento, buscando também reduzir falsos positivos e negativos;

4.8.1.1.3 Executar simulações de ataque que compõem hipóteses a serem validadas no processo de caçada contínua de ameaças e gerar registros (logs) e evidências para a busca nas ferramentas envolvidas no processo;

4.8.1.1.4 A CONTRATADA deve, de forma continuada e periódica:

4.8.1.1.4.1 Identificar e entender os ativos-alvo mais críticos e representativos para aplicação dos testes de segurança automatizados;

4.8.1.1.4.2 Criar e configurar os casos de uso, processos, ciclos e cobertura de testes;

4.8.1.1.4.3 Administrar e monitorar a execução dos testes, analisar e reportar os resultados e recomendações decorrentes;

4.8.1.1.4.4 Configurar e calibrar a Solução de testes de segurança de forma a otimizar a eficácia das detecções e alertas e reduzir o tempo médio para detecção (MTTD) e o tempo médio de reparo (MTTR) das falhas de segurança;

4.8.1.1.4.5 O licenciamento da solução ofertada deverá abranger todo o parque da CONTRATANTE, possibilitando a instalação de seus agentes em todas as máquinas, ainda que sejam realizadas simulações em apenas 60 (sessenta) ativos por mês;

4.8.1.1.4.6 Criar e melhorar painéis (dashboards) e relatórios personalizados para apresentar resultados objetivos e abrangentes.

4.8.1.2 Para realização das simulações de ataque deve ser entregue uma ferramenta com as seguintes características:

4.8.1.2.1 Os itens que compõem a Solução de BAS e seu sistema de gerenciamento devem ser produzidos pelo mesmo fabricante;

4.8.1.2.2 Não serão aceitos componentes baseados em software projetados para uso genérico, devendo estes serem providos por fabricantes amplamente consolidados no mercado. Como referência de mercado serão adotados estudos de institutos de análise independente e imparcial, como Gartner, Forrester, IDC, ISG Group;

4.8.1.2.3 A solução deve contemplar a versão de software e/ou firmware mais estável e recomendado pelo fabricante;

4.8.1.2.4 O fabricante deve possuir rede de inteligência (threat inteligence) própria da solução para atualização constante de ameaças (threat feed) de forma automática;

4.8.1.2.5 Permitir o gerenciamento centralizado da ferramenta, por meio de interface gráfica (GUI), nos formatos web segura (https) ou em formato de aplicativo cliente compatível com Windows 10 e superior, podendo ser em nuvem (cloud), appliance virtual ou por meio da própria solução;

4.8.1.2.6 Sendo a gerência em cloud (nuvem), o encaminhamento de dados deve ser criptografado e protegido, sem enviar dados dos usuários e armazenados de forma criptografada.

4.8.1.2.7 Quanto à arquitetura, a solução deverá:

4.8.1.2.7.1 Possuir agentes (softwares que possam ser instalados em máquinas, ou em ambientes virtuais (servidores), confeccionadas para simulação de ataques ou apresentar atores simuladores) virtuais, podendo ser arquivos *.OVA , com a capacidade de criar um local próprio capaz de permitir a reprodução de ataques;

4.8.1.2.7.2 Possuir agentes compatíveis com sistemas operacionais Linux e Windows (Server e 10);

4.8.1.2.7.3 Possibilitar a instalação de agentes, ou máquinas OVA/ ISO em ambientes de cloud (nuvem).

4.8.1.2.8 Quanto as principais características, a solução deverá:

4.8.1.2.8.1 Ser capaz de simular ataques em gateways de web e e-mail, web application firewall (WAF), em endpoints (EDR, Antivírus), simular ataques em toda a cadeia de destruição cibernética (Cyber Kill Chain), incluindo infiltração, movimento lateral e exfiltração de dados, phishing, ransomwares, violações de segurança e ataques persistentes avançados (APTs);

4.8.1.2.8.2 Não trazer qualquer risco real de infectar a rede do cliente em suas atividades;

4.8.1.2.8.3 Ter seu portfólio de ataques baseado em frameworks de segurança cibernética, tais como MITRE ATTACK, OWASP, CVSS e NIST;

4.8.1.2.8.4 Possuir portfólio de ataques, templates ou cenários que deverá ser atualizado continuamente, de forma manual e automática, com a opção de agendar a atualização em determinado período;

4.8.1.2.8.5 Possibilitar a configuração de cenários de ataque, permitindo a seleção de quais ataques executar no teste;

4.8.1.2.8.6 Permitir o agendamento de simulações com a opção de execução contínua e automatizada;

4.8.1.2.8.7 Possibilitar a execução ilimitada de todos os vetores de simulação disponíveis pela plataforma durante a vigência do mesmo;

4.8.1.2.8.8 Possuir base ampla de recomendação de remediação possibilitando visualizar ações de correção, redução do impacto da vulnerabilidade/ataque e prevenção alinhados com as recomendações específicas dos fabricantes de elementos de segurança;

4.8.1.2.8.9 Possuir atualização diária da base de malwares;

4.8.1.2.8.10 Possuir a instrumentação de IoCs (Indicators of Compromise) provenientes de provedores de Threat Intelligence e/ou laboratório de inteligência de ameaça do fabricante da solução;

4.8.1.2.8.11 Possuir simulações de campanhas de ameaças, com link para o relatório da identificação e descrição da ameaça em campo, descrevendo seus impactos e identificando as regiões do mundo afetadas pela campanha;

4.8.1.2.8.12 Disponibilizar APIs (Application Programming Interfaces) que permitam sua integração com demais soluções de segurança;

4.8.1.2.8.13 Possuir integração nativa com soluções de SIEM;

4.8.1.2.8.14 Possuir integração com linguagens de script ou Python;

4.8.1.2.8.15 Possuir integração nativa com soluções de EDRs.

4.8.1.2.9 Quanto aos dashboards, a solução deverá:

4.8.1.2.9.1 Possuir dashboard com visualização dos resultados das simulações que retratem o nível de risco para cada fase da “Cyber Kill Chain”, baseado no MITRE ATT&CK com a possibilidade de customizar as visões apresentadas.

4.8.1.2.9.2 Apresentar dados históricos de diferentes ataques simulados, bem como a visão de rastreamento;

4.8.1.2.9.3 Detalhar:

Tipo de ataque simulado;

O que o artefato executou;

Data em que a simulação do ataque aconteceu;

Taxa de penetração.

4.8.1.2.9.4 Permitir a realização de backup ou a opção de recuperação da solução, em caso de desastre, para no mínimo as configurações da solução de BAS. Podendo ser funcionalidade não disponível para o cliente, realizado sob demanda junto ao fabricante.

4.8.1.2.10 Quanto aos relatórios e logs a solução deverá:

4.8.1.2.10.1 Apresentar relatórios e registros de auditoria detalhados, que identifiquem o histórico completo de acessos (logins) e ações, por cada usuário ou grupo de usuários;

4.8.1.2.10.2 Ter a opção de gerar relatórios após cada avaliação comparando com o resultado de testes anteriores, mostrando as vulnerabilidades mais críticas;

4.8.1.2.10.3 Permitir exportar relatórios para no mínimo no formato PDF ou CSV (Comma-separated values);

4.8.1.2.10.4 Apresentar relatório detalhando a ação do ataque simulado;

4.8.1.2.10.5 Permitir exportar os logs da solução via API ou conectores compatíveis com o SIEM;

4.8.1.2.10.6 Ser capaz de criar incidentes de forma manual e automática por meio de integrações com o SIEM.

4.9 TREINAMENTO NAS TECNOLOGIAS PROPOSTAS

4.9.1 A CONTRATADA deverá aplicar treinamento técnico para a equipe da CONTRATANTE, incluindo todas as tecnologias propostas.

4.9.2 O treinamento poderá ser realizado de forma presencial ou remota (desde que de forma síncrona, com instrutor ao vivo).

4.9.3 O treinamento deverá ter carga horária mínima de 40 horas, distribuídas em sessões práticas e teóricas.

4.9.4 A CONTRATADA deverá fornecer material didático digital, incluindo slides, apostilas e exercícios práticos.

4.9.5 O(s) instrutor(es) deverá(ão) possuir certificação e experiência comprovada de, no mínimo, 1 ano em operação da(s) plataforma(s) apresentada(s).

5. ACORDO DE NÍVEL DE SERVIÇO:

5.1. A CONTRATADA deverá atender aos níveis de serviços mínimos visando assegurar a qualidade do serviço prestado, que deve ser aferido mensalmente por ferramenta automatizada e validada pelo responsável técnico da CONTRATANTE.

5.2. Na tabela abaixo, constam os indicadores de qualidade a serem adotados para edição de qualidade e incidência de glosas, quando aplicável:

Indicador de qualidade	Meta Exigência	Fonte de dados	Cálculo de Glosa
Disponibilidade do Link de dados	99,7%	Ferramenta de monitoramento	2% Valor do serviço mensal + (1% * tempo de indisponibilidade minutos)

Indicador de qualidade	Meta Exigência	Fonte de dados	Cálculo de Glosa
Disponibilidade da infraestrutura do SOC Ativo/Passivo	99,7%	Ferramenta de monitoramento	2% Valor do serviço mensal + (1% * tempo de indisponibilidade minutos)
Disponibilidade das soluções de SIEM/SOAR	99,7%	Ferramenta de monitoramento	2% Valor do serviço mensal + (1% * tempo de indisponibilidade minutos)
Ativos de IT monitorados	100%	Lista de inventários, Ferramenta de ITSM	2% Valor do serviço mensal + (% de ativos descobertos)
Cumprimento dos prazos de 1º atendimento dos chamados	100%	Ferramenta de ITSM	0,5% Valor do serviço mensal * número de chamados
Cumprimento dos prazos de resolução dos chamados	100%	Ferramenta de ITSM	0,5% Valor do serviço mensal * número de chamados
Tempo de detecção de incidentes de segurança	< 20 minutos	Ferramenta de gestão de segurança	0,5% Valor do serviço mensal * número de incidentes
Tempo de comunicação e resposta de incidentes	< 20 minutos	Ferramenta de gestão de segurança	0,5% Valor do serviço mensal * número de incidentes
Tempo de resposta de vulnerabilidades	< 20 minutos	Ferramenta de gestão de segurança	0,5% Valor do serviço mensal * número de incidentes
Tempo de registro e documentação dos incidentes e eventos relevantes	< 60 minutos	Ferramenta de ITSM	0,5% Valor do serviço mensal * número de incidentes
Qualificação do profissional	100%	Atualização de certificações e experiência profissional dos funcionários alocados, apuração trimestral	2% do valor serviço mensal * número de profissional sem qualificação
Eficácia e Eficiência	100%	Atrasos nas Entrega de relatórios ou de baixa qualidade da informação	2% do valor do serviço mensal

Tabela - Acordo de serviço e glosa

5.3. Para fins de controle das atividades, deverá ser utilizada a ferramenta de ITSM da CONTRATANTE, para registro de todos os chamados;

5.4. Todos os chamados deverão ser classificados, quanto ao nível de severidade da demanda:

- **Critica**: 1º atendimento em até 2 horas e resolução em até 4 horas - Ocorre quando há incidentes de segurança que impactam no negócio ou produção da

CONTRATANTE, causados pela perda ou paralisação total do serviço. Os chamados de severidade “Crítica” não poderão ser interrompidos até o completo restabelecimento do serviço envolvido, mesmo que se estenda por períodos noturnos, dias úteis e não úteis.

- **Alta**: 1º atendimento em até 4 horas e resolução em até 8 horas - Ocorre quando existe uma grave indisponibilidade ou perda de funcionalidade do serviço. Os chamados de severidade “Alta” não poderão ser interrompidos até o completo restabelecimento dos serviços envolvidos.
- **Média**: 1º atendimento em até 8 horas e resolução em até 24 horas – Ocorre quando existe uma perda menor de serviço. Os chamados de severidade “Média” devem contar com esforço concentrado da CONTRATADA até aplicar solução ou medida de contorno.
- **Baixa**: 1º atendimento em até 24 horas e resolução em até 48 horas - Ocorre quando não existe perda de funcionalidade Os chamados de severidade “Baixa” serão atendidos dentro do prazo.

5.5. Todos os chamados devem ser classificados, quanto ao tipo de demanda:

I. **Requisição/solicitação de serviços**: são demandas formalizadas que solicitam alguma tarefa específica, tais como confecção de relatórios de segurança, solicitação de análise de alguma vulnerabilidade, pedido de testes de penetração pontuais em aplicação ou infraestrutura, avaliação de segurança de alguma aplicação, atualização de bases de ameaça, configuração de solução de segurança, dentre outras.

II. **Incidentes**: são eventos ou ocorrências que comprometam a confidencialidade, integridade ou disponibilidade de informações e sistemas alvos de proteção no Datacenter, tais como: eventos intencionais ou acidentais, tais como: ataques cibernéticos, como invasões de rede, “ransomware”, “phishing”, entre outros; Extravio ou roubo de informações; Problemas de hardware ou software, como falhas de sistema ou corrupção de dados, dentre outros.

III. **Demandas diversas**: são aquelas que refletem o registro de ações diárias, semanais ou mensais da equipe de segurança de informação. Por exemplo,

aquelas demandas que necessitam ser executadas de forma contínua para o correto monitoramento e detecção. São chamados sem impacto para os usuários finais.

IV. **Projetos de segurança**: são aquelas mais complexas, que demandam mais tempo de estudo, análise e arquitetura de eventual solução de segurança, incluindo um plano de mudanças, em que envolva a atuação de várias equipes da CONTRATANTE.

5.6. Deverá ser aberto um chamado para cada vulnerabilidade, evento de risco ou incidente ou problema reportado ou detectado de forma manual ou automática na ferramenta de ITSM da CONTRATANTE;

5.7. Os prazos para 1º atendimento e resolução dos chamados de qualquer tipo e severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado pela CONTRATADA e/ou CONTRATANTE, recebendo dela uma identificação para acompanhamento, controle e histórico;

5.8. Os chamados deverão ser concluídos até que a solução definitiva ou de contorno aceitável seja estabelecida através da interação entre as partes;

5.9. O fechamento do chamado classificados como projeto, o gerente da CONTRATADA, deverá coordenar junto ao Responsável Técnico da CONTRATANTE, poderá se dar quer pela recomendação e/ou aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema com o menor risco;

5.10. Um chamado fechado sem anuência do Responsável técnico da CONTRATANTE ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas;

5.11. O somatório das glosas é limitado ao percentual máximo de 30% (trinta por cento) do valor de faturamento mensal. Quando houver superação do percentual máximo, o gestor do contrato deverá ser notificado para aplicação de sanções administrativas previstas no contrato.

5.12. Em caso de cenário de crise, e que não seja possível a apuração do acordo de nível de serviço, devido a indisponibilidade dos serviços críticos e houver prejuízos a

contratante, ficará a Contratada sujeita às glosas e à aplicação das sanções administrativas previstas em Contrato sem prejuízo de outras

5.13. A CONTRATADA deverá entregar mensalmente relatório constando os chamados abertos e atendidos durante o período, contendo os dados de número dos chamados, tipo da demanda, descrição, severidade, data e hora de abertura, data e hora de início do atendimento, data e hora de conclusão, descrição da resolução adotada e demais evidências ou relatório das ferramentas de gestão de segurança.

5.14. Caberão sanções administrativas, os seguintes desvios:

- Uso indevido de credencial e permissão de acesso aos recursos de TI da CONTRATADA, sem os devidos respaldos técnicos
- Realizar mudança na infraestrutura sem que haja uma requisição de mudança devidamente aprovação pela CONTRATANTE
- Fraudar, manipular, descaracterizar indicadores/meta de nível de serviço, descritos na tabela acima;
- Causar qualquer indisponibilidade dos serviços, dano físico aos equipamentos ou danos lógicos ou perda de informações da CONTRATANTE, por motivo de erros operacionais na execução das atividades deste documento.

5.15. Para atestação da nota fiscal e/ou fatura, é condicionada a entrega do relatório mensal, e planilha de indicadores de qualidade, para fins de pagamento dos serviços executados.

6. DA QUALIFICAÇÃO TÉCNICA

6.1. Prova de aptidão da empresa licitante para desempenho de atividade pertinente e compatível com o objeto da licitação, por meio de certidão(ões) ou atestado(s), fornecido(s) por pessoa jurídica de direito público ou privado, podendo ser apresentados em nome da matriz ou da filial do fornecedor;

6.1.1 A LICITANTE disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados e comprovação técnica em até 5 dias úteis, apresentando, quando solicitado pela CONTRATANTE, cópia do contrato que deu suporte à contratação,

endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos;

6.1.2 Considera-se compatível com o objeto da licitação a apresentação de atestado de capacidade técnica que comprove a prestação de serviço para no mínimo 50% do quantitativo previsto no ITEM 3.8.2 deste Termo de Referência;

6.1.3 Será admitida a soma dos atestados ou certidões apresentados pelas licitantes, desde que estes sejam tecnicamente pertinentes e compatíveis em características, quantidades e prazos com o objeto da licitação.

6.1.4 Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução;

6.1.5 Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:

6.1.5.1 Identificação da empresa ou órgão contratante, bem como da empresa contratada, ambas com sua razão social, número do CNPJ e endereço;

6.1.5.2 Descrição dos serviços que foram realizados;

6.1.5.3 Período de execução dos serviços;

6.1.5.4 Assinatura do responsável legal, com local e data.

6.2 A CONTRATADA deverá apresentar, no momento da habilitação, certificados válidos e documentação de vínculo com profissionais qualificados com as principais soluções de segurança usadas pela CONTRATANTE:

- Tenable Certified Analyst (ou certificação equivalente reconhecida pelo fabricante);
- Trend Micro Certified Professional (para EDR/XDR);
- Akamai Certified Microsegmentation Administrator ou equivalente da solução Guardicore.

6.3 A LICITANTE deverá ser parceira oficial do(s) fabricante(s) da(s) tecnologia(s) proposta(s), sendo tal comprovação realizada através de carta oficial do(s) (fabricante);

6.4 A licitante deverá comprovar o vínculo com estes profissionais por meio de cópia da carteira de trabalho, registro de empregados ou quaisquer outros documentos, que comprove o vínculo empregatício, no momento da assinatura do contrato, com as certificações:

- Ter no mínimo 02 (dois) profissionais certificados na solução de Detecção e Resposta a Incidentes de Segurança adotada, com, no mínimo, 12 (doze) meses de experiência em monitoramento de segurança (SOC).
- Ter pelo menos 01 (um) profissional Analista ou Engenheiro de Segurança Especializado em Pentest, com no mínimo 12 (doze) meses de experiência em testes de invasão.

6.5 A LICITANTE deverá possuir as seguintes certificações internacionais de segurança da informação e privacidade de dados:

5.8.1 ISO/IEC 27001 (Segurança da Informação);

5.8.2 ISO/IEC 27701 (Privacidade da Informação).

A certificação ISO 27001 é um selo de qualidade reconhecido globalmente, indicando que o SOC segue as melhores práticas em segurança da informação.

6.6 A LICITANTE deverá entregar declaração quanto às questões de confidencialidade e responsabilidade dos produtos gerados a aderência às normas ABNT ISO/IEC NBR 27001:2013 e ABNT ISO/IEC NBR 27002:2013.

6.7 A LICITANTE deverá entregar declaração quanto a possuir uma Política de Segurança da Informação e seus controles, entre eles, desde Segurança Física, Controle de Acesso, até a Gestão de Continuidade de Negócios.

6.8 O ambiente da licitante vencedora, será objeto de diligência, para verificar o cumprimento das exigências constantes neste documento, antes da homologação da licitante, previamente agendado, observando o prazo máximo de 10 dias úteis para homologação.

6.9 A proposta apresentada deve ser complementada por planilha “ponto a ponto” de comprovação do atendimento da especificação das soluções

informatizadas, indicando a documentação técnica (manual técnico, catálogo técnico, datasheet, folha de dados ou folha de especificações, artigo de conhecimento de suporte técnico e similares do fabricante), a página e/ou tópico onde se encontra cada informação, ou, alternativamente, imagens da console das soluções que comprovem o atendimento do requisito.

7 PROVA DE CONCEITO

7.1 O pregoeiro poderá, subsidiado pelo apoio técnico e como condição de aceitação da proposta, solicitar à LICITANTE classificada em primeiro lugar que se submeta à realização de uma Prova de Conceito - POC para comprovar o pleno atendimento de requisitos para os quais restem eventuais dúvidas, a serem enumerados pela CONTRATANTE.

7.1.1 O pregoeiro irá agendar data e horário, com antecedência de até 10 (dez) dias úteis, para que a LICITANTE apresente a prova de conceito;

7.1.2 Qualquer alteração de data e horário será devidamente informada no chat, podendo ocorrer postagens diárias;

7.1.3 A POC será realizada em ambiente preparado pela licitante e apresentada de forma on-line, para que demonstre a comprovação do atendimento dos requisitos enumerados, conforme as especificações exigidas no edital e seus anexos;

7.1.4 Serão de inteira responsabilidade da LICITANTE todas as despesas para a preparação e apresentação da POC;

7.1.5 A LICITANTE que não apresentar a POC na data estabelecida, ou que apresentar POC que não atenda às exigências do edital, terá sua proposta desclassificada.

8. DA FUNDAMENTAÇÃO LEGAL DA CONTRATAÇÃO

7.6 A presente contratação tem fundamento na Lei Federal n.º 13.303/2016, no Decreto Municipal n.º 44.698/2018, no Regulamento de Licitações e Contratos da IPLANRIO – RLC IPLANRIO, disponível no Portal da Prefeitura do Rio de

Janeiro: https://iplanrio.prefeitura.rio/contratos-e-licitacoes/, bem como nas regras procedimentais acerca da modalidade de pregão eletrônico, dispostas na Lei Federal n.º14.133/2021.

8 DAS OBRIGAÇÕES DA CONTRATANTE

8.6 Acompanhar e fiscalizar a execução do contrato;

8.7 Anotar em registro próprio todas as ocorrências relacionadas com a execução, sob os aspectos quantitativos e qualitativos, comunicando quaisquer fatos que exijam medidas corretivas por parte da CONTRATADA;

8.8 Atestar as Faturas /Notas Fiscais;

8.9 Efetuar os pagamentos devidos nos prazos estabelecidos;

8.10 Realizar os pagamentos na forma e condições previstas;

8.11 Realizar a fiscalização do objeto deste Termo de Referência;

8.12 Devolver, com a devida justificativa, qualquer item entregue fora das especificações.

8.13 Manter o cadastro das pessoas que poderão efetuar abertura e autorizar fechamento de chamados.

8.14 Fornecer, revogar os acessos e informações relacionadas aos ativos a serem protegidos e monitorados durante a vigência do contrato.

9 DAS OBRIGAÇÕES DA CONTRATADA

São obrigações da CONTRATADA:

10.1 Realizar os serviços de acordo com todas as exigências contidas no Termo de Referência e na proposta;

10.2 Tomar as medidas preventivas necessárias para evitar danos a terceiros, em consequência da execução dos serviços;

10.3 Responsabilizar-se integralmente pelo ressarcimento de quaisquer danos e prejuízos, de qualquer natureza, que causar à CONTRATANTE ou a terceiros, decorrentes da execução do objeto desta contratação, respondendo por si, seus empregados, prepostos e sucessores, independentemente das medidas

preventivas adotadas e da comprovação de sua culpa ou dolo na execução do contrato;

10.4 Atender às determinações e exigências formuladas pela CONTRATANTE;

10.5 Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, efeitos ou incorreções resultantes da execução ou de materiais empregados, no prazo determinado pela Fiscalização;

10.6 Responsabilizar-se, na forma do Contrato, por todos os ônus, encargos e obrigações comerciais, sociais, tributárias, trabalhistas e previdenciárias, ou quaisquer outras previstas na legislação em vigor, bem como por todos os gastos e encargos com material e mão de obra necessária à completa execução dos serviços:

10.6.1 em caso de ajuizamento de ações trabalhistas contra a CONTRATADA, decorrentes da execução do presente Contrato, com a inclusão do Município do Rio de Janeiro ou da CONTRATANTE como responsável subsidiário ou solidário, a CONTRATANTE poderá reter, das parcelas vincendas, o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

10.6.2 no caso da existência de débitos tributários ou previdenciários, decorrentes da execução do presente Contrato, que possam ensejar responsabilidade subsidiária ou solidária da CONTRATANTE, as parcelas vincendas poderão ser retidas até o montante dos valores cobrados, que serão complementados a qualquer tempo com nova retenção em caso de insuficiência;

10.6.3 as retenções previstas nas alíneas “a” e “b” poderão ser realizadas tão logo tenha ciência o Município do Rio de Janeiro ou a CONTRATANTE da existência de ação trabalhista ou de débitos tributários e previdenciários e serão destinadas ao pagamento das respectivas obrigações caso o Município do Rio de Janeiro ou entidade da Administração Pública indireta sejam compelidos a tanto,

administrativa ou judicialmente, não cabendo, em nenhuma hipótese, ressarcimento à CONTRATADA;

10.6.4 eventuais retenções previstas nas alíneas “a” e “b” somente serão liberadas pela CONTRATANTE se houver justa causa devidamente fundamentada.

10.7 Manter as condições de habilitação e qualificação exigidas para a contratação durante todo prazo de execução contratual;

10.8 Responsabilizar-se, na forma do Contrato, pela qualidade dos serviços executados e dos materiais empregados, em conformidade com as especificações do Termo de Referência, com as normas da Associação Brasileira de Normas Técnicas – ABNT, e demais normas técnicas pertinentes, a ser atestada pelos responsáveis pela fiscalização da execução do contrato, assim como pelo refazimento do serviço e a substituição dos materiais recusados, sem ônus para o(a) CONTRATANTE e sem prejuízo da aplicação das sanções cabíveis;

10.9 Responsabilizar-se inteira e exclusivamente pelo uso regular de marcas, patentes, registros, processos e licenças relativas à execução desta contratação, eximindo a CONTRATANTE das consequências de qualquer utilização indevida;

10.10 Indicar, nas notas fiscais emitidas, quando o objeto envolver prestação de serviços, o efetivo período do mês que está sendo faturado.

10.11 Durante a vigência do contrato, a CONTRATADA deverá informar à CONTRATANTE, eventuais alterações na relação de quadro de profissionais alocados e habilitados para a execução do serviço.

10.12 Em casos de ataque legítimo, a CONTRATADA deverá disponibilizar profissionais capacitados para atuarem de forma presencial no LOCAL da CONTRATANTE, visando o restabelecimento do ambiente, incluindo todas as despesas para deslocamento, hospedagem, alimentação e demais custos para o cumprimento deste item, sem ônus para a CONTRATANTE.

10.13 A CONTRATADA deverá prover soluções de continuidade de prestação de serviços, em relação à não interrupção dos serviços, para diversos casos:

10.14 Assegurar, nos casos de greve ou paralisação de seus colaboradores, a continuação da prestação dos serviços, por meio da execução de plano de

contingência, inclusive nos casos de greve ou paralisação dos transportes públicos, hipótese em que deverá promover, às suas expensas, os meios necessários para que seus colaboradores cheguem aos seus locais de trabalho.

10.15 Ao longo do contrato a Contratada ficará obrigada a promover, gradativamente, a transição contratual, com transferência de tecnologia e técnicas empregadas, sem perda de informações, capacitando, se solicitado, os técnicos da CONTRATANTE ou os da nova pessoa jurídica que continuará a execução dos serviços, sem ônus para a Contratante.

10.16 Reportar aos responsáveis da CONTRATANTE, imediatamente, qualquer anormalidade, erro ou irregularidade que possa comprometer a execução dos serviços e o bom andamento das atividades da Contratante, observando as demais obrigações da Contratada.

9. FORMA DE DISPONIBILIZAÇÃO

9.1. As licenças deverão ser disponibilizadas caso sejam necessárias, por meio eletrônico.

10. PERÍODO DE ESTABILIZAÇÃO

10.1. Os primeiros 90 (noventa) dias corridos após o início da execução dos serviços serão considerados como período de estabilização e ajustes dos serviços prestados, desde que a CONTRATADA não recuse a obtenção de nenhuma Ordem de Serviço.

10.2. Neste período, os resultados esperados e os níveis de qualidade exigidos não serão aplicados, oportunizando a CONTRATADA realizar os devidos ajustes.

11. SUBCONTRATAÇÃO

11.1. É vedada a subcontratação.

12. DOS PRAZOS E VIGÊNCIA

12.1. O prazo de validade da Ata de Registro de Preços será de 12 (doze) meses.

12.2. A contratação terá eficácia a partir da data da publicação do instrumento correspondente no Diário Oficial do Município do Rio de Janeiro e vigorará por 24 (vinte e quatro) meses, podendo ser prorrogado, nos termos da legislação em vigor.

12.3. Os prazos de execução dos serviços poderão ser prorrogados ou alterados nos termos do Decreto Municipal nº 44.698/2018 e do Regulamento de Licitações e contratos da IPLANRIO;

12.4. O prazo de garantia dos serviços realizados será o mesmo da vigência do contrato.

12.5. No caso de serviços continuados, o contrato poderá ser prorrogado por até 5 (cinco) anos, na forma do Decreto Municipal n.º 44.698/18 e do Regulamento de Licitações e contratos da IPLANRIO.

13. DA GARANTIA CONTRATUAL

13.1. A CONTRATADA prestará garantia de 2% (dois por cento) do valor total do Contrato, como determina o art. 457 do RGCAF, a ser prestada antes do ato de assinatura, em uma das modalidades previstas no art. 445 do RGCAF e no art. 81 do Decreto Municipal n.º 44.698/2018. Seus reforços poderão ser igualmente prestados nas mesmas modalidades. Caso o fornecedor escolha a modalidade seguro-garantia, esta deverá incluir a cobertura das multas eventualmente aplicadas, e, caso escolha a modalidade carta-fiança, deverá observar as regras específicas eventualmente existentes e informadas pela Contratante.

13.2. No caso de seguro-garantia, o instrumento deverá contemplar a possibilidade de sua renovação no período compreendido entre a data de assinatura do contrato e a data de encerramento da sua execução e incluir a cobertura dos valores relativos a multas eventualmente aplicadas;

13.3. No caso de fiança bancária, deverá ser observado o padrão estabelecido pelo Decreto Municipal nº 26.244/06 ou pela Portaria IPLANRIO “N” Nº 153, de 09 de fevereiro de 2011;

13.4. A licitante vencedora deverá apresentar a garantia no prazo de até 05 (cinco) dias úteis, contados da convocação por meio de comunicação formal;

13.4.1. A não-observância do prazo estabelecido caracteriza o descumprimento total da obrigação assumida, sujeitando a licitante vencedora às penalidades legalmente estabelecidas.

13.5. O (A) CONTRATANTE utilizará a garantia para assegurar as obrigações associadas ao contrato, podendo recorrer a esta inclusive para cobrar valores de multas eventualmente aplicadas e ressarcir-se dos prejuízos que lhe forem causados em virtude do descumprimento das referidas obrigações. Para reparar esses prejuízos, poderá a CONTRATANTE ainda reter créditos.

13.6. Os valores das multas impostas por descumprimento das obrigações assumidas no contrato serão descontados da garantia caso não venham a ser quitados no prazo de 03 (três) dias úteis, contados da ciência da aplicação da penalidade. Se a multa aplicada for de valor superior ao valor da garantia prestada, além da perda desta, responderá A CONTRATADA pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente;

13.7. Em caso de rescisão decorrente de falta imputável à CONTRATADA, a garantia reverterá integralmente ao CONTRATANTE, que promoverá a cobrança de eventual diferença que venha a ser apurada entre o importe da garantia prestada e o débito verificado;

13.8. Na hipótese de descontos da garantia a qualquer título, seu valor original deverá ser integralmente recomposto no prazo de 7(sete) dias úteis, exceto no caso da cobrança de valores de multas aplicadas, em que esse será de 48 (quarenta e oito) horas, sempre contados da utilização ou da notificação pelo (a) CONTRATANTE, o que ocorrer por último, sob pena de rescisão administrativa do contrato;

13.9. Caso o valor do contrato seja alterado, art. 92 do Decreto Municipal n.º 44.698/18, A CONTRATADA deverá complementar o valor da garantia para que seja mantido o percentual de 2% (dois por cento) do valor do contrato;

13.10. Sempre que houver reajuste ou alteração do valor do contrato, a garantia será complementada no prazo de 7 (sete) dias úteis do recebimento, pela CONTRATADA, do correspondente aviso, sob pena de aplicação das sanções previstas no RGCAF;

13.11. Os reforços do valor da garantia poderão ser igualmente prestados em uma das modalidades previstas no art. 81 do Decreto Municipal 44.698/18;

13.12. A garantia contratual somente será restituída após o integral cumprimento do contrato, mediante ato liberatório da autoridade CONTRATANTE, nos termos do artigo 465, do RGCAF, podendo ser retida, se necessário, para quitar eventuais obrigações da CONTRATADA.

14. DA GARANTIA DOS PRODUTOS E SERVIÇOS

14.1. Além das garantias contratuais previstas em lei, os serviços e licenças fornecidos, são de responsabilidade da CONTRATADA:

14.1.1. Garantir a IPLANRIO que os serviços disponibilizados não infrinjam quaisquer patentes, direitos autorais ou segredos de negócios (trade-secrets);

14.1.2. Manter os serviços contratados dentro dos parâmetros definidos em sua contratação;

14.1.3. Se comprometer a reparar, corrigir ou refazer, serviços que não estiverem dentro dos padrões definidos, às suas expensas, em um período de até 90 (noventa) dias.

15. DO LOCAL DA PRESTAÇÃO DOS SERVIÇOS

15.1. Os serviços do centro de operação de segurança serão prestados remotamente, salvo em casos de ataque legítimo, onde deverá ser prestado presencial, para resposta ao incidente e restabelecimento dos serviços prestados;

15.2. Para prestação dos serviços remoto, a CONTRATADA deve disponibilizar comunicação dedicada, através de conectividade (LPCD), com capacidade adequada ao tráfego de rede, para interligação a rede da CONTRATANTE, por meio de conexão ponto a ponto, de acordo com os requisitos de segurança definidos pela CONTRATANTE.

16. CRONOGRAMA FÍSICO-FINANCEIRO

16.1. Mediante a necessidade de implantação do serviço para efetivo início da execução do serviço contínuo e mensal do Centro de Operação de Segurança (SOC), segue o cronograma de desembolso físico-financeiro:

16.1.1. O pagamento relativo ao item 1, da "Tabela do Objeto do Termo de Referência" deste Termo de Referência será realizado de forma integral após o aceite da CONTRATANTE relacionado à implantação dos agentes de coleta e integrações para início do serviço de SOC. Essa fase deverá ter o prazo de entrega até 60 dias após a assinatura de contrato;

16.1.2. O pagamento relativo ao item 2, da "Tabela do Objeto do Termo de Referência" deste Termo de Referência serão realizados, em duas parcelas, sendo:

17.1.2.1 60% (sessenta por cento) do valor total quando decorrida a assinatura do contrato entre a CONTRATADA e CONTRATANTE contemplando o licenciamento de softwares utilizados no projeto.

17.1.2.2 40% (cinquenta por cento) do valor total em parcelas mensais após o término da implantação das integrações com as soluções existentes para início do serviço de SOC. Essa fase deverá ter o prazo de entrega até 30 dias após o relatório de conclusão do item 01;

16.1.3. O pagamento relativo ao item 3, da "Tabela do Objeto do Termo de Referência" deste Termo de Referência será realizado de forma integral após o aceite da CONTRATANTE relacionado à entrega do referido item.

17. DA FISCALIZAÇÃO E ACEITE DO OBJETO

17.1. A CONTRATADA submeter-se-á a todas as medidas e procedimentos de fiscalização. Os atos de fiscalização, inclusive inspeções e testes, executados pela CONTRATANTE e/ou por seus prepostos, não eximem A CONTRATADA de suas

obrigações no que se refere ao cumprimento das normas, especificações e projetos, nem de qualquer de suas responsabilidades legais e contratuais;

17.2. A Fiscalização da execução do (s) serviço (s) caberá à comissão designada por ato da autoridade competente no âmbito da Empresa Municipal de Informática S/A - IPLANRIO. Incumbe à Fiscalização a prática de todos os atos que lhe são próprios nos termos da legislação em vigor, respeitados o contraditório e a ampla defesa.

17.3. A CONTRATADA declara, antecipadamente, aceitar todas as decisões, métodos e processos de inspeção, verificação e controle adotados pela CONTRATANTE, se obrigando a fornecer os dados, elementos, explicações, esclarecimentos e comunicações de que este necessitar e que forem considerados necessários ao desempenho de suas atividades;

17.4. A CONTRATADA se obriga a permitir que o pessoal da fiscalização da CONTRATANTE acesse quaisquer de suas dependências, possibilitando o exame das instalações e também das anotações relativas aos equipamentos, pessoas e materiais, fornecendo, quando solicitados, todos os dados e elementos referentes à execução do contrato;

17.5. Compete à CONTRATADA fazer minucioso exame dos serviços, de modo a permitir, a tempo e por escrito, apresentar à Fiscalização, para o devido esclarecimento, todas as divergências ou dúvidas porventura encontradas e que venham a impedir o bom desempenho do contrato. O silêncio implica total aceitação das condições estabelecidas;

17.6. A atuação fiscalizadora em nada restringe a responsabilidade única, integral e exclusiva da CONTRATADA no que concerne aos serviços executados, à sua entrega e às consequências e implicações, próximas ou remotas, perante a CONTRATANTE, ou perante terceiros, do mesmo modo que a ocorrência de eventuais irregularidades na execução contratual não implicará corresponsabilidade da CONTRATANTE ou de seus prepostos;

17.7. A aceitação do objeto deste Termo de Referência se dará mediante a avaliação de Comissão de Fiscalização designada pela autoridade competente no âmbito da CONTRATANTE, e constituída na forma do art. 501, do RGCAF, que

constatará se os serviços prestados atendem a todas as especificações contidas neste Termo de Referência ou no processo que ensejou a presente contratação;

17.8. O objeto do presente Termo de Referência será recebido em tantas parcelas quantas forem às relativas ao pagamento;

17.9. Os serviços cujos padrões de qualidade estejam em desacordo com a especificação deste Termo de Referência e seus anexos deverão ser recusados pela Comissão responsável pela fiscalização do contrato, que anotará em registro próprio as ocorrências e determinará o que for necessário à regularização das faltas ou defeitos observados. No que exceder à sua competência, comunicará o fato à autoridade superior, em 5 (cinco) dias, para ratificação;

17.10. Na hipótese de recusa de aceitação, por não atenderem às exigências da CONTRATANTE, A CONTRATADA deverá re-executar os serviços recusados, passando a contar os prazos para pagamento e demais compromissos da CONTRATANTE da data da efetiva aceitação. Caso A CONTRATADA não substitua os bens não aceitos no prazo assinado, a CONTRATANTE se reserva o direito de providenciar o seu fornecimento às expensas da CONTRATADA, sem prejuízo das penalidades cabíveis;

18. DAS CONDIÇÕES DE PAGAMENTO

18.1. Os pagamentos serão efetuados à CONTRATADA, conforme descrito no item 17 - Cronograma Físico-Financeiro, após a regular liquidação da despesa, nos termos do art. 63 da Lei Federal nº 4.320/64, observada a regras de recebimento do objeto contidas no RLC IPLANRIO e neste Termo de Referência. O prazo para pagamento será de 30 (trinta) dias, contados da data do protocolo do documento de cobrança no setor competente do(a) CONTRATANTE e obedecido o disposto na legislação.

18.2. Para fins de medição, se for o caso, e faturamento, o período-base de medição do serviço prestado será de um mês, considerando-se o mês civil, podendo no primeiro mês e no último, para fins de acerto de contas, o período se constituir em fração do mês, considerado para esse fim o mês com 30 (trinta) dias.

18.3. O pagamento à CONTRATADA será realizado em razão dos serviços efetivamente prestados e aceitos no período-base mencionado no item anterior sem que o(a) CONTRATANTE esteja obrigado(a) a pagar o valor total do Contrato tendo como referência o cronograma físico-financeiro descrito no item 18 deste Termo de Referência.

18.4. A CONTRATADA deverá apresentar juntamente com o documento de cobrança, os comprovantes de recolhimento do FGTS e INSS de todos os empregados atuantes no contrato, assim como Certidão Negativa de Débitos Trabalhistas – CNDT ou Certidão Positiva de Débitos Trabalhistas com efeito negativo válida, declaração de regularidade trabalhista

18.5. O valor dos pagamentos eventualmente efetuados com atraso, desde que não decorra de fato ou ato imputável à CONTRATADA, sofrerá a incidência de juros calculados de acordo com a variação da Taxa Selic, pro rata die entre o 31º (trigésimo primeiro) dia da data do protocolo do documento de cobrança no setor competente da CONTRATANTE e a data do efetivo pagamento, limitado ao percentual de 12% (doze por cento) ao ano.

18.6. O valor dos pagamentos eventualmente antecipados será descontado à taxa de 1% (um por cento) ao mês, calculada pro rata die, entre o dia do pagamento e o 30º (trigésimo) dia da data do protocolo do documento de cobrança no setor competente do (a) CONTRATANTE.

18.7. O pagamento será efetuado à CONTRATADA através de crédito em conta bancária do fornecedor cadastrado junto à Coordenação do Tesouro Municipal.

19. DAS SANÇÕES ADMINISTRATIVAS

19.1. Sem prejuízo de indenização por perdas e danos, a CONTRATANTE poderá impor ao contratado, pelo descumprimento total ou parcial das obrigações a que esteja sujeito, as seguintes sanções, observado o Regulamento Geral do Código de Administração Financeira e Contabilidade Pública do Município do Rio de Janeiro – RGCAF, o Decreto Municipal n.º 44.698/2018 e o

Regulamento de Licitações e Contratos da CONTRATANTE, garantida a defesa prévia ao contratado:

I - Advertência;

II - Multa de mora de até 1% (um por cento) por dia útil sobre o valor do Contrato ou do saldo não atendido do Contrato;

III - Multa de até 20% (vinte por cento) sobre o valor do Contrato ou do saldo não atendido do Contrato, conforme o caso, e, respectivamente, nas hipóteses de descumprimento total ou parcial da obrigação, inclusive nos casos de rescisão por culpa da CONTRATADA;

IV - Suspensão temporária do direito de licitar e impedimento de contratar com a Administração Municipal.

19.2. A multa aplicada será depositada em conta bancária indicada pela IplanRio, descontada dos pagamentos eventualmente devidos, descontada da garantia ou cobrada judicialmente.

19.3. As sanções previstas nos incisos I e IV do subitem 20.1 poderão ser aplicadas juntamente com as dos incisos II e III, devendo a defesa prévia do interessado, no respectivo processo, ser apresentada no prazo de 10 (dez) dias úteis e não excluem a possibilidade de rescisão unilateral do contrato;

19.4. Do ato que aplicar a pena prevista no inciso IV do subitem 20.1, a autoridade competente no âmbito da CONTRATANTE dará conhecimento aos demais órgãos e entidades municipais interessados, na página oficial desta empresa pública na internet.

19.5. A sanção prevista no inciso IV do subitem 20.1 poderá também ser aplicada às empresas ou aos profissionais que, em razão dos contratos regidos pelo Decreto Municipal n.º 44.698/2018:

I - Tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

II - Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

III - demonstrem não possuir idoneidade para contratar com a IplanRio em virtude de atos ilícitos praticados.

19.6. As multas previstas nos incisos II e III do subitem 20.1 não possuem caráter compensatório, e, assim, o pagamento delas não eximirá a CONTRATADA de responsabilidade pelas perdas e danos decorrentes das infrações cometidas.

19.7. As multas aplicadas poderão ser compensadas com valores devidos à CONTRATADA mediante requerimento expresso nesse sentido.

19.8. Ressalvada a hipótese de existir requerimento de compensação devidamente formalizado, nenhum pagamento será efetuado à CONTRATADA antes da comprovação do recolhimento da multa ou da prova de sua relevação por ato da Administração, bem como antes da recomposição do valor original da garantia, que tenha sido descontado em virtude de multa imposta, salvo decisão fundamentada da autoridade competente que autorize o prosseguimento do processo de pagamento.

20. DA MATRIZ DE RISCOS

20.1. Para a presente contratação foram identificados os principais riscos conhecidos na Matriz constante do Anexo I deste Termo de Referência, bem como estabelecidos os respectivos responsáveis e descritas suas respostas sugeridas.

20.2. É vedada a celebração de aditivos decorrentes de eventos supervenientes alocados na Matriz de Riscos como sendo de responsabilidade da CONTRATADA.

20.3. Sempre que atendidas as condições do contrato e mantidas as disposições da Matriz de Risco, considera-se mantido o equilíbrio econômico-financeiro.

20.4. A proposta comercial deverá ser elaborada levando em consideração a natureza e a extensão dos riscos relacionados na Matriz de Risco.

21. DA PROPOSTA DE PREÇOS

21.1. A pretensa CONTRATADA deverá apresentar proposta de preços

de acordo com as especificações deste Termo de Referência e nos moldes praticados pelo Município do Rio de Janeiro.

21.2. Os preços propostos deverão estar de acordo com os praticados no mercado, em moeda nacional (Reais) e neles deverão estar inclusos todos os impostos, taxas, fretes, material, mão de obra, instalações e quaisquer outras despesas necessárias e não especificadas neste Termo de Referência, mas julgadas essenciais ao cumprimento do objeto desta contratação.

22. DO TIPO DE LICITAÇÃO

22.1. O tipo de licitação será o menor preço Global.

23. DA PROTEÇÃO DE DADOS PESSOAIS

23.1. Havendo tratamento de dados pessoais no desenvolvimento de quaisquer atividades relacionadas com o objeto, as Partes observarão a Legislação de Privacidade e de Proteção de Dados Pessoais, em especial, a Lei 13.709/2018 (LGPD).

23.2. As partes se comprometem a tratar os Dados Pessoais necessários à execução das atividades previstas neste termo, única e exclusivamente para cumprir com a finalidade a que se destinam, respeitando toda legislação aplicável sobre segurança da informação, privacidade e proteção de dados, incluindo, mas não se limitando à Lei nº 13.709/2018 (“Lei Geral de Proteção de Dados Pessoais”).

23.3. Para fins deste termo:

(I) “Dados Pessoais" significam todas as informações tratadas pelas Partes em razão deste termo em qualquer forma tangível ou intangível, ou que pessoalmente identifiquem ou tornem

identificáveis quaisquer dos seus empregados, clientes, agentes, usuários finais, fornecedores, contatos ou representantes;

(II) “Dados Pessoais Sensíveis” são quaisquer dados que disponham sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, ou dado genético ou biométrico, ou dados que, apesar de separadamente não serem sensíveis, possam, em conjunto, resultar em informação sensível quando vinculado à pessoa natural;

(III) “Tratamento” significa toda operação realizada com Dados Pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, compartilhamento, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

23.4. As Partes devem garantir a implementação de medidas técnicas e administrativas aptas a manter a integridade, confidencialidade, disponibilidade e segurança dos dados pessoais tratados, sempre considerando a natureza de cada um deles, assim como o nível de risco potencial a que estiverem expostos.

23.5. É expressamente proibido copiar, transferir ou de outra forma compartilhar Dados Pessoais de qualquer natureza para plataformas externas à originalmente utilizada, comprometendo-se as Partes a garantir que seus diretores, gerentes, funcionários e colaboradores cumpram com tal restrição, salvo por acordo escrito entre as Partes, hipótese na qual será requerida a apresentação de garantias suficientes que os Dados Pessoais extraídos sejam utilizados dentro das finalidades previstas, e de que a extração ou interconexão pretendida atenda aos critérios mínimos de segurança e confiabilidade estabelecidos pela Parte controladora.

23.6. As Partes asseguram que, caso os Dados Pessoais sejam tratados por terceiros (incluindo subcontratados, agentes autorizados, filiadas, coligadas, subsidiárias, controladora e controladas):

(I) os terceiros estão obrigados a ter níveis de proteção aos Dados Pessoais iguais ou superiores aos estabelecidos neste termo;
(II) os terceiros somente poderão realizar o tratamento para atender a(s) finalidade(s) para a(s) qual(is) o dado foi originalmente coletado e/ou compartilhado. De qualquer forma, as Partes, independentemente de estarem na condição de operador ou controlador, serão responsáveis, no limite disposto pela legislação aplicável, pelas ações e omissões realizadas por tais terceiros relativas ao Tratamento dos Dados Pessoais;
(III) a contratada deverá submeter à anuência prévia da contratante a realização de subcontratação ou suboperação, restringindo-se ao estritamente
necessário para o fiel desempenho da execução das atividades previstas no presente termo, permanecendo a contratada integralmente responsável por garantir a sua observância perante a contratante.

Parágrafo Quarto - Quando existirem operações de Tratamento de Dados Pessoais Sensíveis ou tratamento de dados relacionados a crianças e adolescentes, a Parte envolvida deve garantir que as medidas técnicas e administrativas apropriadas e aptas a manter a integridade, confidencialidade, disponibilidade e segurança destas informações sejam implementadas, incluindo, mas não se limitando, às operações de criptografia.

Parágrafo Sexto - As Partes deverão ainda:

(I) tomar medidas razoáveis para informar suas equipes de trabalho sobre as responsabilidades resultantes da Lei Geral de Proteção de Dados Pessoais;
(II) No caso de tratamento de dados sensíveis, deverá ser comprovada pela contratada a existência de política interna de privacidade e proteção de dados pessoais, bem como o treinamento e atualização do seu corpo de funcionários mediante comprovação específica;
(III) notificar prontamente a outra Parte por escrito, bem como aos titulares dos dados e à ANPD, quando cabível, sempre que souber ou suspeitar que ocorreu um incidente de segurança com dados pessoais, ou uma violação à Lei Geral de Proteção de Dados Pessoais;
(IV) investigar incidentes de segurança com dados pessoais, tomando todas as medidas necessárias para eliminar ou conter eventual exposição, bem como quaisquer danos que possam recair sobre a outra Parte, inclusive cooperando com os esforços de investigação e remediação, se comprometendo, ainda, a fornecer os documentos e informações necessários para mitigar eventuais danos à outra Parte;
(V) envidar esforços razoáveis para garantir a integridade, disponibilidade e confidencialidade das informações tratadas em todas as circunstâncias;
(VI) manter devidamente atualizados os registros das operações de Tratamento de Dados Pessoais, que conterá a categoria dos dados tratados, os agentes de tratamento envolvidos na atividade, qual a finalidade das diversas atividades de Tratamento realizadas e por quanto tempo os Dados

Pessoais serão processados e armazenados para o cumprimento de sua finalidade originária;
(VII) garantir que os registros das operações de Tratamento de Dados Pessoais deverão estar disponíveis para assegurar eventual auditoria ou diligência por
parte da contratante;
(VIII) assegurar que os dados pessoais tratados em razão da finalidade celebrada neste instrumento permaneçam corretos e devidamente atualizados, devendo as
informações desatualizadas serem imediatamente corrigidas ou excluídas;
(IX) cooperar mutuamente e razoavelmente na definição de uma solução para implementar os novos requisitos de proteção e segurança de Dados Pessoais,
caso assim a legislação vier a exigir.

Parágrafo Sétimo - As Partes se comprometem ainda a:

a) não reter quaisquer Dados Pessoais fornecidos pela outra Parte por um período superior ao necessário para o cumprimento de sua finalidade nos termos do presente
instrumento e/ou para o cumprimento das suas obrigações legais, conforme permitido pela lei aplicável;
b) colaborar mutuamente visando o integral cumprimento das disposições previstas na Lei Geral de Proteção de Dados Pessoais;
c) tratar Dados Pessoais apenas nos locais estabelecidos pelas Partes, qual seja, (território nacional ou apontar o país).

Parágrafo Oitavo - As Partes se comprometem ainda a se auxiliarem no atendimento das requisições realizadas por titulares de dados, providenciando, de forma imediata, ou no máximo em 72 (setenta e duas) horas:

(I) a confirmação da existência do Tratamento;
(II) o acesso aos Dados Pessoais tratados;
(III) a correção dos Dados Pessoais incompletos, inexatos ou desatualizados;
(IV) a anonimização, o bloqueio ou a eliminação dos Dados Pessoais;
(V) a portabilidade dos Dados Pessoais;
(VI) a informação sobre as entidades públicas e privadas com as quais foi realizado o compartilhamento de dados, bem como o atendimento aos pressupostos legais para tal compartilhamento, na forma dos arts. 24, parágrafo único e 26, §1° da LGPD;
(VII) a informação das consequências da revogação do consentimento;
(VIII) Registro de pedido de revogação do consentimento e sua implementação;
(IX) a informação dos fatores que levaram a uma decisão automatizada e sobre a possibilidade de recurso em face dela.

Parágrafo Nono - A critério da CONTRATANTE e do seu encarregado de dados, a CONTRATADA poderá ser instada a auxiliar a CONTRATANTE na elaboração de relatórios de impacto à proteção de dados pessoais, observado o disposto nos arts. 5°, XVII e 38 da LPGD, no âmbito da execução deste ajuste.

Parágrafo Décimo - As Partes concordam ainda em auxiliar e prestar suporte uma à outra, sem que tal ação transforme responsável a parte que apenas está prestando suporte e auxílio, no caso de reclamações, danos, responsabilidades, despesas, multas e perdas resultantes do Tratamento, ou qualquer outra situação que exija o pagamento de valores pecuniários, desde que os eventos que levaram a tais consequências guardem qualquer relação com:

(I) falha de uma das Partes, ou de terceiros por esta contratada, em cumprir com as disposições expostas neste instrumento;

(II) exposição acidental ou proposital de Dados Pessoais;

(III) omissão ou negligência de uma das Partes ou de terceiros por esta contratada em cumprir com as disposições expostas neste instrumento.

Rio de Janeiro, 14 de julho de 2025.

_____

Leonardo Cavalieri

Matrícula: 40/622.627-9

Gerente de Segurança Cibernética

IPLANRIO/DOP

_____

Jorge Francisco Antunes da Silva

Matrícula: 40/2622163-4

Diretor de Operações

IPLANRIO

ANEXO I – Matriz de Risco

ANEXO I - MATRIZ DE RISCOS – REGISTRO DE PREÇOS PARA PRESTAÇÃO DE SERVIÇO DE CENTRO DE OPERAÇÃO DE SEGURANÇA (SOC)										
Identificação dos Riscos					**Análise Qualitativa**			**Resposta aos Riscos (Tratamento)**		
Id.	**Tipo**	**Risco**	**Categoria**	**Sub Categoria**	**P**	**I**	**P x I**	**Estratégia**	**Resposta Sugerida**	**Responsável**
R001	Ameaça	Devido a variação cambial, pode haver aumento dos custos dos produtos importados	Organizacional	Aquisição	8	8	**64**	Mitigar	A contratada deverá considerar a variação cambial em sua proposta de preço	Contratada
R002	Ameaça	Devido ao calendário orçamentário da PCRJ, pode haver atraso no pagamento do contrato	Organizacional	Aquisição	7	9	**63**	Mitigar	A contratada deverá manter fluxo de caixa para cobrir o período descoberto	Contratada
R004	Ameaça	Devido a alteração da política econômico-financeira, pode haver aumento nos tributos após a contratação	Organizacional	Aquisição	4	5	**20**	Aceitar Ativamente	A contratada deverá buscar alternativas para cumprimento do contrato	Contratada
R005	Ameaça	Monitoramento do ambiente, devido à ausência de mão de obra qualificada e operação 24horas por 7 dias	Organizacional	Aquisição	9	9	**81**	Mitigar	Ampliar quadro técnico e capacitar para grupo de trabalho com foco exclusivo na monitoração com regime 24hx7d	Contratante
R006	Ameaça	Devido ao atraso de pagamento do contrato, a equipe da contratada poderá levar ao atraso no atendimento do serviço	Organizacional	Aquisição	7	8	**56**	Mitigar	Deverá manter fluxo de caixa para cobrir o período descoberto	Contratada

ANEXO II – TERMO DE PRIVACIDADE E RESPONSABILIDADE

Declaro para os devidos fins e efeitos, que me responsabilizo integralmente pela adequada utilização dos dados pessoais a que tiver acesso, estando ciente de que posso vir a ser responsabilizado civil, criminal e administrativamente pelos danos morais ou materiais decorrentes da utilização, reprodução ou divulgação indevida dos dados sobre os deveres, requisitos e responsabilidades decorrentes da Lei n. 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais – LGPD, sobre as formas de coleta, tratamento e compartilhamento de dados.

Declaro conhecimento sobre as 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; e de que a responsabilidade de qualquer pessoa que intervenha em uma das fases abrangidas pelo fluxo dos dados pessoais subsiste mesmo após o término do tratamento.

Rio de Janeiro, _____ de _____ de _____

_____

Nome:

Documento:

ANEXO III – TERMO DE CIÊNCIA E VISTORIA

Declaro, para fins de participação e habilitação no Pregão Eletrônico nº_____ (PA nº_____), que a empresa _____, CNPJ_____ representada por_____, vistoriou o(s) local (is) de realização dos serviços, tomando pleno conhecimento da área de abrangência, da complexidade e de todas as peculiaridades técnicas e elementos necessários à elaboração da proposta comercial e à execução dos trabalhos integrantes do Edital do presente Pregão.

Rio de Janeiro - RJ, ___ de _____de 2025.

_____

Representante da Iplanrio

_____

Representante da licitante:

Documento: