Governo do Estado do Rio de Janeiro
Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro
Diretoria de Segurança da Informação

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

1. OBJETIVO

1.1. O presente Termo de Referência tem por objetivo descrever a **Contratação de empresa de Tecnologia da Informação para o fornecimento de solução de segurança para proteção de dispositivos finais (antivírus), aplicações em nuvem, servidores de e-mail e detecção/resposta unificada a eventos de segurança que envolvam a solução, contemplando o treinamento para operacionalização e o suporte técnico para as soluções contratada**s.

1.2. A licitação será realizada em âmbito nacional, via Sistema de Registro de Preços, na modalidade PREGÃO em sua forma eletrônica, nos termos da Lei nº 10.520/2002 (Regulamenta o art. 37, inciso XXI, da Constituição Federal, para instituir a modalidade de licitação denominada pregão), da Lei nº 8.666/1993 (Regulamenta o art. 37, inciso XXI, da Constituição Federal, que institui normas para licitações e Contratos da Administração Pública e dá outras providências) e do Decreto Estadual nº 46.751/2019 (Regulamenta o Sistema de Registro de Preços no âmbito Estadual.

1.3. Forma de adjudicação do objeto: **MENOR PREÇO** global por lote.

1.4. Forma de execução do objeto: **Empreitada por preço unitário**.

2. JUSTIFICATIVAS

2.1. O PRODERJ, instituição vinculada à Secretaria de Estado de Transformação Digital, atua como Órgão Gestor da Tecnologia da Informação e Comunicação, no âmbito do Governo do Estado do Rio de Janeiro, na forma do art. 5º, do Decreto nº 47.278/2020, que altera a estrutura organizacional do Poder Executivo e reestrutura o Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC.

2.2. É responsável por sediar, manter e operar a TIC do Estado, ou seja, os sistemas de informações, o desenvolvimento de sistemas, as bases de dados de vários Órgãos estaduais e os diversos equipamentos hospedados no Data Center do Estado. É responsável também por prover serviços de Internet aos Órgãos da administração estadual, tais como correio eletrônico, consultoria, desenvolvimento e hospedagens de páginas, portais, intranets e extranets, bem como conduzir e disponibilizar as atas de registro de preços e contratos corporativos para suprir itens relativos à TIC aos Órgãos e entidades do Estado.

2.3. Também tem por competência o Registro de Preços em contratações de bens e serviços relativos à Tecnologia da Informação e Comunicação, para o atendimento das demandas dos demais órgãos da administração direta e indireta da Administração Pública Estadual, conforme o art. 4º,§2º do Decreto nº 46.751/2019, que regulamenta o Sistema de Registros de Preços no Estado do Rio de Janeiro, bem como o art. 5º, XVII, do Decreto nº 47.278/2020, já citado.

2.4. Diante dessas atribuições e devido ao crescente número de tentativas de invasão e violação de dados, o PRODERJ desenvolveu estudos técnicos com a finalidade de propor uma solução de proteção de endpoints (qualquer “dispositivo final” em uma rede, tais como notebooks, desktops, smartfones, tablets, servidores, entre outros, sejam eles físicos ou virtualizados). Uma solução para proteção de endpoint, amiúde denominada antivírus, é uma ferramenta de primeira necessidade em segurança cibernética, sobretudo no âmbito corporativo e é o recurso de segurança da informação mais tradicional disponível no mercado.

2.5. Atualmente, quase a totalidade das políticas e dos serviços públicos são ofertados, direta ou indiretamente, através de sistemas tecnológicos, que proporcionam acesso rápido à informação, bem como um atendimento menos burocrático às demandas dos cidadãos. Esta realidade, contudo, traz riscos ao Governo Estadual, enquanto prestador de tais serviços e guardião de informações importantes, sobretudo dados pessoais dos cidadãos, razão pela qual deve se precaver para a proteção dessas informações e também para a manutenção do funcionamento ininterrupto dos seus serviços.

2.6. Essa preocupação com a segurança dos dados se torna ainda mais relevante com o aumento na utilização de recursos como a comunicação por VPN para realização de trabalho home office, gerando um grande fluxo de dados na rede do governo, muito diferente do habitual. Tal cenário é considerado um legado do período pandêmico da COVID19 (2020/2021), quando as corporações se viram obrigadas a utilizar recursos que viabilizassem o trabalho remoto, uma vez que a circulação de pessoas foi reduzida por razões sanitárias

2.7. A segurança cibernética é fundamental para o perfeito funcionamento dos serviços prestados pelo Estado, cuja responsabilidade inclui registros, cadastros, integrações, acessos, inclusões, guardas e tratamentos de informações públicas e privadas dentro do ambiente tecnológico, o que torna os órgãos da Administração Pública, alvos constantes de cyber ataques.

2.8. O aumento do uso de dispositivos móveis e de dispositivos de armazenamento através de interfaces externas como a USB, bem como a propagação do uso de computação e armazenamento em nuvem, fez com que a segurança de perímetro se tornasse insuficiente para garantir a segurança em redes de dados locais. Os dispositivos de segurança como firewalls de rede, filtros webs, IDS e IPS não garantem mais a segurança plena da informação dentro dessas redes locais, sendo necessário que, cada estação de trabalho ou servidor que esteja conectado à rede, consiga prover mecanismos de segurança para si mesmo, e, com isso, contribuir para a garantia da segurança da rede como um todo. Daí a relevância da adoção de solução de segurança para proteção desses dispositivos.

2.9. Tem-se observado nos últimos tempos, um crescimento no número de tentativas de violação de dados aos ambientes tecnológicos, através de contaminações por vírus, malwares e suas variantes, bem como outros tipos de ameaças cibernéticas junto aos computadores e demais dispositivos que acessam a rede tecnológica de todo o Estado, colocando em sérios riscos o sigilo, a integridade e disponibilidade das informações.

2.10. Segundo o *Relatório de Inteligência de Ameaças DDoS*, da Netscout System, empresa especializada em cibersegurança, o Brasil é o principal alvo de ataques cibernéticos na América Latina. O país concentra 39,23% das ocorrências de ciberataques do tipo DDoS sofridos na região no segundo semestre de 2022.

2.11. Assim como os ataques cibernéticos estão em constante evolução, as camadas de proteção e detecção precisam evoluir para garantir a segurança do ambiente.

2.12. Ataques direcionados e as ameaças avançadas são os mais recentes métodos utilizados por cyber criminosos para se infiltrarem na infraestrutura das redes. Esses ataques têm a característica dominante de serem altamente customizados ou personalizados com base no que se pode obter de

informações acerca do alvo. As informações são obtidas, em sua maioria, por buscas na internet ou através de engenharia social, com tamanha sofisticação que essas ameaças conseguem evadir as defesas convencionais e permanecerem ocultas enquanto roubam dados corporativos.

2.13. Desde 2015 o Governo federal vem dando publicidade à Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal, como um importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, cujo objetivo foi de melhorar a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais. Assim, vem impulsionando as discussões sobre o tema no âmbito da Administração Pública federal, bem como nos demais entes federados.

2.14. Nesse passo, a segurança dos endpoints é bastante abordado no âmbito da Estratégia Nacional de Segurança Cibernética (E-Ciber), instituída pelo Decreto Federal nº 10.222 de 2020, que em seu anexo, parte II "Análise dos Eixos Estratégicos", no item 1.3. "Proteção Estratégica", aponta justamente a preocupação com a proteção desses ativos. Saliente-se que o E-Ciber do governo federal tem servido de elemento norteador aos demais entes da federação, na propositura de suas políticas de cibersegurança.

2.15. A almejada contratação proporcionará melhores condições de prevenir possíveis incidentes, melhorando os níveis de segurança dos serviços prestados pelos órgãos da Administração Pública Estadual.

3. ALINHAMENTO ESTRATÉGICO

3.1. Eventual contratação para a solução objeto deste Termo de Referência encontra alinhamento estratégico com o Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC 2023, do PRODERJ, conforme descrito em sua página 33:

- Objetivo Estratégico 7 - Promover o processo de Segurança da Informação e Comunicação: Implementar o processo, revisar normas, monitorar os incidentes de segurança e disseminar a cultura da segurança da informação junto aos servidores do PRODERJ e demais Órgãos da Administração Pública Estadual. (objetivo não orçamentário)

3.2. Também encontra alinhamento com o Plano Plurianual (PPA) 2020- 2023, registrada com o código de ação nº 1293 (atualização tecnológica do parque computacional), e código do produto nº 6884 (ferramenta de segurança da informação implantada).

3.3. Caberá ao setor competente providenciar a inclusão do objeto no PCA- Plano de Contratações Anual.

4. DOTAÇÃO ORÇAMENTÁRIA

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

5. DETALHAMENTO DO OBJETO

5.1. Requisitos objetivos da contratação

5.1.1. A presente demanda visa a disponibilização de solução de segurança que faça a proteção de dispositivos, com o objetivo de auxiliar os órgãos da Administração a mitigar diversas ameaças de segurança que afetam a rede governo, bem como obter os seguintes benefícios:

a) Melhorar as ações de segurança da informação no âmbito da Administração Pública;

b) Implementar mecanismos sofisticados para proteção de dados sensíveis;

c) Aumentar o grau de confidencialidade da segurança da informação;

d) Assegurar o provimento de Infraestrutura de TIC segura e adequada para as nossas áreas finalísticas;

e) Contribuir para a garantia da confidencialidade, integridade e disponibilidade das informações produzidas e armazenadas em meios tecnológicos;

f) Aumentar a segurança dos sistemas;

g) Robustecer e ampliar os quesitos de segurança das estações de trabalho, servidores e dispositivos móveis contra ameaças cibernéticas, melhorando a atual gestão de incidentes de segurança da informação;

h) Possuir maior capacidade de identificar acessos indevidos, obtendo maior agilidade e efetividade no bloqueio desses acessos;

i) Gerar dados e informações para maior eficiência das equipes de tratamento e resposta a incidentes, de modo a auxiliar em auditorias de incidentes de segurança;

j) Proporcionar maior aderência com a legislação e orientações relacionadas à proteção de dados pessoais e a segurança das informações.

5.2. Requisitos de Negócio

5.2.1. Proteção dos endpoints corporativos, aplicações de nuvem e servidores de e-mail, com a disponibilização de plataforma centralizada para o controle e correlação de informações dos agentes da solução instalados nos dispositivos.

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

5.3. Requisitos Legais

A contratada deverá se sujeitar, no que couber, ao quanto disposto na Lei nº 9.609/98 - Lei de Software.

5.4. Requisitos de Manutenção

Todas as rotinas para fins de manutenção com vistas ao pleno e adequado funcionamento da solução ao longo da vigência contratual estará a cargo da CONTRATADA na forma do Suporte Técnico previsto no subtópico 5.7 deste documento. O referido Suporte Técnico contempla a manutenção corretiva com o objetivo solucionar defeitos encontrados no software, e também a manutenção evolutiva na forma da atualização oportuna dos softwares contratados.

5.5. Requisitos de Segurança da Informação e Privacidade

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

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

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

5.5.4. A CONTRATADA deverá assinar Termo de Confidencialidade e Sigilo na forma do modelo do Anexo IV deste documento.

5.5.5. A CONTRATADA deve atender às Políticas de Segurança da Informação e demais normativos correlatos publicados pela CONTRATANTE.

5.6. **Necessidades tecnológicas**

Os requisitos tecnológicos da solução encontram-se no Anexo I - Especificações Técnicas do Objeto.

5.6.1. **Instalação e configuração**

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

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

5.6.1.3. Ficam desde já considerados os seguintes aspectos referentes à etapa de instalação e configuração dos softwares e/ou aplicativos (itens 1, 2, 3, 4, 5, 6 e 7 do lote) a serem entregues pela CONTRATADA, na infraestrutura da CONTRATANTE, bem como migração das regras existentes, se assim for o caso:

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

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

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

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

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

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

VII - Para instalação e configuração devem ser consideradas as seguintes premissas:

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

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

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

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

5.6.1.5. No caso do contrato contemplar o fornecimento do item nº 07 do lote, a referida reunião de kick-off servirá inclusive para que sejam definidos os detalhes da prestação do serviço que compõe aquele item. Nesta possibilidade, serão definidas na reunião o escopo de ativos críticos para monitoramento, definição de alertas e outros possíveis requisitos para a devida prestação do referido serviço.

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

5.7. **Suporte técnico**

5.7.1. As especificações de suporte técnico constantes deste subtópico, vigorarão para os itens nº 01 ao nº 06 do lote (subscrições de licença de software).

5.7.2. Durante todo o período contratual, a Contratada será responsável pelo suporte técnico das soluções tecnológicas que compõem o objeto.

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

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

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

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

5.7.7. Todos os prazos para atendimento do suporte começarão a ser contados a partir da abertura do chamado no sistema.

5.7.8. O suporte técnico deverá contemplar manutenção corretiva e evolutiva para as soluções contratadas, e não poderá acarretar custos adicionais à CONTRATANTE.

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

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

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

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

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

5.7.14. A contratada será responsável por possíveis migrações para novas versões da solução oferecida, sempre que demandadas pela CONTRATANTE.

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

5.7.16. **Critérios de Medição do Suporte Técnico**

Nível de Severidade dos Chamados		
Categoria	**Nível**	**Descrição**
Urgente	1	Serviços totalmente indisponíveis. Falha em servidor de produção que deixe indisponíveis os recursos do mesmo (serviço parado). Impacto a múltiplos usuários e/ou falha em servidor de produção que afete operações críticas da Contratante
Crítico	2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta no acesso aos aplicativos. Falha intermitente em serviços suportados que torne o ambiente inoperante. Impacto individual ou a pequenos grupos. Operação normal afetada, mas sem interrupção.
Normal	3	Serviços disponíveis com ocorrência de alarmes e avisos, consulta sobre problemas, dúvidas gerais sobre a ferramenta antivírus. Manutenção e monitoramento de eventos de falhas ou de avisos relatados pelo cliente. Pequeno impacto a um ou mais usuários. A correção pode ser feita de forma agendada, em um momento futuro, desde que não afete a segurança do ambiente de rede da Contratante.

Tabela de Prazos de Atendimento ao Suporte				
Modalidade	**Prazos de Atendimento**	**Níveis de Severidade**		
		1. Urgente	**2. Crítico**	**3. Normal**
On site e/ou remoto	Início	1 hora	5 horas	24 horas
	Término	6 horas	10 horas	48 horas
Atualizações e aplicações diversas	Início	Após a disponibilização pelo fabricante		
	Término	24h após atualização da solução		
Indisponibilidade	Total	1 hora para o reestabelecimento do serviço		
	Parcial	3 horas para o reestabelecimento do serviço por completo		

I - A contratada deverá cumprir prazos máximos para respostas aos acionamentos de suporte técnico, de acordo com o nível de severidade de cada chamado, conforme a tabela acima;

II - O descumprimento nos prazos acima descritos poderá implicar a aplicação das sanções do tópico 33 deste Termo de Referência e demais sanções legais;

III - Para os fins do inciso anterior, serão considerados os cr itérios do Acordo de Níveis de Serviços constante do tópico 19 deste documento, para o cálculo de eventuais aplicações de glosas/multas;

IV - A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

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

VI - As multas relativas à sanção, por não cumprimento do nível de serviço, referentes ao suporte técnico serão tratadas em processo apartado, resguardada a ampla defesa e o contraditório e descontadas no valor da garantia, conforme disposto no subtópico 26.3 "b" deste documento.

5.8. **Necessidades socioambientais**

O fornecedor deverá, no que for aplicável ao cumprimento do objeto, obedecer aos critérios estabelecidos no Decreto estadual 43.629/2012.

5.9. **Aderência a padrões e modelos**

Não se aplica.

5.10. **Providências a serem adotadas pela Administração previamente à elaboração do contrato**

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

5.11. **Recursos materiais e humanos**

5.11.1. Em observação ao entendimento do Enunciado nº 14, item 5 da Procuradoria-Geral do Estado do Rio de Janeiro - PGE/RJ, saliente-se que o objeto da presente contratação não prevê o uso de mão de obra residente/dedicada nas dependências do órgão contratante. Adicionalmente registre-se que o objeto também não caracteriza, forma alguma, terceirização de atividade-fim do órgão gestor ou dos partícipes, tendo em vista que se trata de contratação, em

regime de subscrição, de licenças de software com sistema de gerenciamento e respectivos cursos de treinamento, bem como suporte técnico específico do fabricante/fornecedor representante, no âmbito da garantia comum de mercado, que estão diretamente relacionado à atuação de profissionais e especialistas nas soluções contratadas, não se confundindo com as atividades inerentes aos referidos órgãos.

5.11.2. Materiais, insumos e acessórios necessários ao perfeito funcionamento da solução deverão ser arcados pela CONTRATADA, sem custos adicionais para a CONTRATANTE.

5.11.3. Não se aplica o fornecimento de uniformes e equipamentos de proteção individual (EPI), observado o subtópico anterior.

5.12. **Capacitação de servidores**

5.12.1. A capacitação compreende os cursos de treinamento dos itens nº 08 ao nº 13 do lote e são opcionais aos órgãos partícipes e aderentes à Ata de Registro de Preços.

5.12.2. O treinamento deverá abranger a operação da solução ofertada. Assim, os treinamentos dos itens nº 08 ao nº 13 correspondem respectivamente às licenças de software dos itens nº 01 ao nº 06 do lote.

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

5.12.4. Deverá ser entregue para a CONTRATANTE a proposta com o conteúdo do treinamento.

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

5.12.6. Deverá ser ministrado por instrutor capacitado na ferramenta, devendo ser comprovado por meio de certificados ou declaração formal de disponibilidade, exigível após a adjudicação, para a execução do contrato, observado o subtópico 15.1.6. deste documento.

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

5.12.8. **Objetivo**

a) Capacitação da contratante para a operacionalização da ferramenta tecnológica.

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

5.12.9. **Métrica**

O curso de treinamento será contratado por aluno (vaga), de forma que órgão partícipe ou aderente ao Sistema de Registro de Preços possa contratar a quantidade de treinamentos mais adequada para sua necessidade.

5.12.10. **Carga horária**

5.12.10.1. Deverá ter carga horária mínima 40 (quarenta) horas.

5.12.10.2. Deverá iniciar no prazo máximo de até 20 dias úteis contados da emissão da ordem de serviço, quando a CONTRATANTE não especificar prazos no documento.

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

5.12.11. **Forma de realização**

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

5.12.12. **Materiais didáticos e acessórios**

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

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

5.12.13. **Conteúdo programático**

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

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

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

6. DEMANDA ESTIMADA E QUANTITATIVO

6.1. Quantitativos do PRODERJ:

LOTE				
ITEM	**ID SIGA**	**DESCRIÇÃO**	**MÉTRICA**	**QUANTIDADE ESTIMADA**
01	181940	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR*) - para estações de trabalho, incluído o suporte técnico (36 meses)	unidade	448
02	181941	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para servidores, incluído o suporte técnico (36 meses)	unidade	992
03	181942	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para dispositivos móveis, incluído o suporte técnico (36 meses)	unidade	34

04	181943	Subscrição de licenças de uso para solução de proteção a aplicações em nuvem. Incluído o suporte técnico (36 meses)	unidade (usuário)	100
05	181944	Subscrição de licenças de uso para solução de Proteção a servidores de e-mail. Incluído o suporte técnico (36 meses)	unidade (suário)	1.000
06	181945	Subscrição de licenças de uso para solução de visibilidade, detecção, investigação e alertas de incidentes (XDR), incluído o suporte técnico (36 meses)	unidade	2.574
07	181952	Serviço gerenciado de detecção e resposta (MDR)	serviço	2.574
08	181946	Serviço de treinamento na solução EDR para estações de trabalho	vaga	12
09	181947	Serviço de treinamento na solução EDR para servidores	vaga	12
10	181948	Serviço de treinamento na solução EDR para dispositivos móveis	vaga	6
11	181949	Serviço de treinamento na solução de proteção a aplicações em nuvem	vaga	12
12	181950	Serviço de treinamento na solução de proteção a servidores de e-mail	vaga	12
13	181951	Serviço de treinamento na solução XDR	vaga	12

6.2. Após a realização de Plano de Suprimentos (PLS SIGA nº 1286/2023), o quantitativo estimado para a contratação passou a ser o seguinte:

LOTE				
ITEM	**ID SIGA**	**DESCRIÇÃO**	**MÉTRICA**	**QUANTIDADE ESTIMADA**
01	181940	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR*) - para estações de trabalho, incluído o suporte técnico (36 meses)	unidade	28.357
02	181941	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para servidores, incluído o suporte técnico (36 meses)	unidade	4.006
03	181942	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para dispositivos móveis, incluído o suporte técnico (36 meses)	unidade	3.269
04	181943	Subscrição de licenças de uso para solução de proteção a aplicações em nuvem. Incluído o suporte técnico (36 meses)	unidade (usuário)	1.005
05	181944	Subscrição de licenças de uso para solução de Proteção a servidores de e-mail. Incluído o suporte técnico (36 meses)	unidade (suário)	4.426
06	181945	Subscrição de licenças de uso para solução de visibilidade, detecção, investigação e alerta de incidentes (XDR). Incluídos o suporte técnico (36 meses)	unidade	37.312
07	181952	Serviço gerenciado de detecção e resposta (MDR)	serviço	37.312
08	181946	Serviço de treinamento na solução EDR para estações de trabalho	vaga	89
09	181947	Serviço de treinamento na solução EDR para servidores	vaga	86
10	181948	Serviço de treinamento na solução EDR para dispositivos móveis	vaga	63
11	181949	Serviço de treinamento na solução de proteção a aplicações em nuvem	vaga	63
12	181950	Serviço de treinamento na solução de proteção a servidores de e-mail	vaga	60
13	181951	Serviço de treinamento na solução XDR	vaga	87

*** Endpoint Detection and Response**

6.3. Quantidades estimadas para cada órgão participante:

LOTE													
Órgão participante4 / endereço de entrega*	**item 01 ID 181940**	**item 02 ID 181941**	**item 03 ID 181942**	**item 04 ID 181943**	**item 05 ID 181944**	**item 06 ID 181945**	**item 07 ID 181952**	**item 08 ID 181946**	**item 09 ID 181947**	**item 10 ID 181948**	**item 11 ID 181949**	**item 12 ID 181950**	**item 13 ID 181951**
CEPERJ - Fund Centro Est. Estat. Pesq. Serv RJ *Avenida Carlos Peixoto, 54 Sala 304, Botafogo - Rio de Janeiro/RJ*	300	30	50	10	10	400	400	10	10	10	10	10	10
PRODERJ - Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro (Órgão Gestor deste SRP) *Rua da Conceição, 69, 24º Andar / 25º Andar - Bairro Centro - Rio de Janeiro/RJ*	448	992	34	100	1.000	2.574	2.574	12	12	6	12	12	12
SEPLAG - Secretaria de Estado de Planejamento e Gestão *Avenida Erasmo Braga, 118, 7º, 8º, 9º e 10º andares, Centro - Rio de Janeiro/RJ*	500	0	0	0	0	500	500	5	0	0	0	0	5

SECEC - SECRETARIA DE ESTADO DE CULTURA E ECONOMIA CRIATIVA *Avenida Presidente Vargas, 1261, Centro - Rio de Janeiro/RJ ou conforme definido pelo órgão*	250	15	0	10	0	275	275	5	5	0	5	0	5
DETRAN - Departamento de Trânsito do Estado do Rio de Janeiro *Endereço de acordo com o órgão*	5.500	650	200	100	10	6.460	6.460	0	0	0	0	0	0
SEDSODH - Secretaria de Estado de Desenvolvimento Social e Direitos Humanos *Avenida Erasmo Braga, 118, 5º e 7º andares, Centro - Rio de Janeiro/RJ*	300	6	0	0	0	306	306	0	2	0	0	0	0
RIOPREVIDENCIA - Fundo Único de Previdência do Estado do Rio de Janeiro *Rua da Quitanda, 106, Centro - Rio de Janeiro/RJ*	700	150	40	200	0	1.090	1.090	5	5	5	5	5	5
SEPM - Secretaria de Estado de Polícia Militar *Rua Carmo Neto, s/nº, Prédio CICC - Bairro Cidade Nova, Rio de Janeiro/RJ*	7.500	700	2.550	50	0	10.800	10.800	12	12	12	12	12	12
GSI - Gabinete de Segurança Institucional do Governo do Estado do Rio de Janeiro *Rua Pinheiro Machado, s/nº - Laranjeiras, Rio de Janeiro/RJ*	200	0	0	0	0	200	200	0	0	0	0	0	0
IPEM-RJ - Instituto de Pesos e Medidas do Estado do RJ *Rua Padre Manoel da Nóbrega, 539, Piedade - Rio de Janeiro/RJ*	200	20	0	0	0	220	220	5	5	0	0	0	5
FUNARJ - Fundação Anita Mantuano de *Artes do Estado do RJ* *Rua da Alfândega, 91, 5.º andar - Centro - Rio de Janeiro/RJ*	10	6	0	0	0	16	16	0	0	0	0	0	0
LOTERJ - Loteria do Estado do Rio de Janeiro *R. Sete de Setembro, 170, Centro - Rio de Janeiro/RJ*	80	3	0	0	0	83	83	2	2	0	0	0	0

RIO SEGURANÇA ISP - Instituto de Segurança Pública *Avenida Presidente Vargas, nº 817 - 16º andar, Centro - Rio de Janeiro/RJ*	80	20	0	0	0	100	100	0	0	0	0	0	0
SEENEMAR - Secretaria de Energia e Economia do Mar do Estado do Rio de Janeiro *Rua Pinheiro Machado, s/nº, Laranjeiras - Rio de Janeiro/RJ*	200	5	20	0	0	225	225	5	5	5	0	0	5
SEGOV - Secretaria de Estado de Governo *Rua Pinheiro Machado, s/n, Laranjeiras, Rio de Janeiro/RJ*	200	200	200	1	0	601	601	6	6	6	6	6	6
DRM - Departamento de Recursos Minerais do Estado do Rio de Janeiro *Rua Mal. Deodoro, 351, Centro -Niterói/RJ*	120	3	25	0	150	298	298	5	2	2	0	2	2
CGE - Controladoria Geral do Estado do Rio de Janeiro *Avenida Erasmo Braga, 118 - 12º e 13º andar - Setor: DGAF - Rio de Janeiro/RJ*	300	50	1	0	1	352	352	0	0	0	0	0	0
PESAGRO RIO - EMPRESA DE PESQUISA AGROPECUÁRIA DO ESTADO DO RIO DE JANEIRO *Alameda São Boaventura, 770, Fonseca - Niterói/RJ ou conforme definido pelo órgão*	130	20	0	0	0	150	150	2	2	0	0	0	2
FSERJ - Fundação Saúde *Rua Barão de Itapagipe, 225, Rio Comprido - Rio de Janeiro/RJ*	3.934	475	80	514	2.955	7.958	7.958	10	10	10	10	10	10
CENTRAL - Companhia Estadual de Engenharia de Transportes e Logística *Avenida Nsa Sra de Copacabana, 493, 5º andar, Copacabana - Rio de Janeiro/RJ*	160	11	5	0	0	176	176	5	5	5	0	0	5
FAPERJ - Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do RJ *Av. Erasmo Braga 118 - 6º andar - Centro - Rio de Janeiro - RJ*	200	50	60	10	200	520	520	1	1	1	1	1	1

FES - Fundo Estadual de Saúde *Rua México, 128, Centro - RJ*	3.500	250	0	0	0	3.750	3.750	0	0	0	0	0	0
SES - Secretaria de Estado de Saúde *Endereço de acordo com o órgão*	3.500	250	0	0	0	0	0	0	0	0	0	0	0
SETD - Secretaria de Estado de Transformação Digital *Rua da Conceição, 69, 25º Andar - Bairro Centro - Rio de Janeiro/RJ*	45	100	4	10	100	258	258	2	2	1	2	2	2
TOTAL	**28.357**	**4.006**	**3.269**	**1.005**	**4.426**	**37.312**	**37.312**	**89**	**86**	**63**	**63**	**60**	**87**

* ou conforme acordado entre o órgão CONTRATANTE e a CONTRATADA

6.4. Quantidades estimadas para adesão por órgãos não participantes:

	LOTE												
PARÂMETRO	**item 01 ID 181940**	**item 02 ID 181941**	**item 03 ID 181942**	**item 04 ID 181943**	**item 05 ID 181944**	**item 06 ID 181945**	**item 07 ID 181952**	**item 08 ID 181946**	**item 09 ID 181947**	**item 10 ID 181948**	**item 11 ID 181949**	**item 12 ID 181950**	**item 13 ID 181951**
Quantidade máxima de contratação por meio de adesão	56.714	8.012	6.538	2.010	8.852	74.624	74.624	178	172	126	126	120	174
Quantidade máxima de contratação por órgão aderente	14.178	2.003	1.634	502	2.213	18.656	18.656	44	43	31	31	30	43

6.4.1. A Ata de Registro de Preços poderá ser aderida por quaisquer órgãos ou entidades do Estado, que não tenham participado do certame licitatório, ora denominados Órgãos Aderentes.

6.4.2. Podem também ser considerados **ÓRGÃOS ADERENTES** os órgãos ou entidades municipais, distritais, de outros estados e federais, resguardadas as disposições de cada ente.

6.4.3. O ÓRGÃO ADERENTE poderá, mediante prévia anuência do ÓRGÃO GERENCIADOR, aderir à Ata de Registro de Preços, desde que realizado estudo que demonstre a viabilidade e a economicidade.

7. LEVANTAMENTO DAS ALTERNATIVAS DE MERCADO

7.1. **Solução 1) Utilização de solução antivírus gratuita proprietária (Microsoft Defender Antivírus)**

- **Vantagens:** O Microsoft Defender Antivírus não envolve custos financeiros diretos, pois é uma solução que já vem embarcada nos sistemas Windows, bastando apenas o dispositivo possuir uma licença válida do sistema operacional, para então utilizar o produto. Em termos de proteção, o antivírus nativo oferece como principais features: Proteção antimalware baseada em assinaturas, firewall de host, controle parental, controle de aplicativos, controle de navegador e controle de integridade do sistema.
- **Desvantagens:** A solução Microsoft embarcada possui apenas uma pequena fração das funcionalidades presentes no escopo do estudo técnico realizado, principalmente no que diz respeito ao gerenciamento centralizado e correlação de eventos de segurança. Há de destacar também que, neste cenário, não haveria um acordo de nível de serviço para o suporte técnico da solução antivírus, pois não haveria nenhum contrato firmado com esta finalidade.

7.2. **Solução 2) Subscrição de Solução EDR, com XDR e outros opcionais**

- **Vantagens:** A ferramenta de "Endpoint Detection and Response/EDR" e outros itens disponibilizados neste cenário representam um salto qualitativo no que diz respeito a proteção de dispositivos finais, se comparada às alternativas gratuitas. O objeto deste cenário pode oferecer todos os recursos de segurança atualmente disponíveis no mercado para a proteção de dispositivos finais.

- **Desvantagens:** Em um cenário de descontinuidade contratual, a Contratante perderia completamente a camada de proteção aos endpoints, já que não possuiria o licenciamento perpétuo da solução.

7.3. **Solução 3) Aquisição de licenças perpétuas de Solução EDR, com garantia e suporte técnico**

- **Vantagens:** Este cenário de contratação preserva as características técnicas dos módulos EDR para Estações de Trabalho e Servidores, e ainda seria capaz de proporcionar uma proteção mínima, em caso de término da garantia, pois manteria ainda algumas das funcionalidades de proteção da ferramenta.

- **Desvantagens:** Por tratar-se de aquisição, o objeto não contaria com a funcionalidade de detecção e resposta estendida, bem como os outros opcionais (proteção a apps de nuvem, servidores de e-mail e MDR), pois estes costumam estar disponíveis para contratação somente na modalidade SaaS. Há de se considerar ainda que a aquisição de uma solução EDR on premise possui requisitos computacionais em sua implementação, ficando a cargo da Contratante garantir a manutenção da infraestrutura utilizada na solução.

7.4. Saliente-se que não foram encontradas soluções de **softwares de uso público**, disponíveis no Portal do Software Público Brasileiro mantido pelo Governo Federal (https://softwarepublico.gov.br/social/search/software_infos?

utf8=%E2%9C%93&utf8=%E2%9C%93&display=&filter=&software_type=all&query=antiv%C3%ADrus&commit=Filtro&software_display=15&sort=rating acesso em 28.09.2023).

8. ANÁLISE DE PROJETOS SIMILARES

Nos estudos técnicos que embasam este Termo de Referência forma observadas contratações similares verificáveis nos certames abaixo listado:

a) Tribunal Regional Federal 1ª Região - Pregão 024/2022;
b) COREN-AM - Pregão Eletrônico Nº 10/2022;
c) Instituto Federal - IFMA - Pregão nº 004/2022;
d) Instituto Chico Mendes - MMA - Pregão nº 037/2022;
e) IPASSP - Município de Santa Maria-RS - Pregão nº 01/2022;
f) Câmara dos Deputados - P.E. nº 117/2022;
g) Ministério da Defesa - Secretaria Geral - Pregão n° 026/2022;
h) Depto. Nacional de Infraestrutura de Transportes - Pregão 00505/2021-000 SRP;
i) Serviços Gráficos de Sergipe - SEGRASE - CONTRATO Nº 011/2022;
j) Agência Nacional de Telecomunicações - ANATEL - Edital nº 24/2022;
k) Escola Superior do Ministério Público da União - P.E. nº 11/2022 - MPU;
l) Ministério da Saúde - Fundação Oswaldo Cruz - FIOCRUZ - Pregão nº 011/2023;
m)Ministério da Saúde - Fundação Nacional de Saúde-DF - Pregão nº 012/2022;
n) Agência Nacional de Saúde - ANS - Edital nº 18/2022;
o) Banco de Brasília - P.E. nº 32/2023;
p) Poder Judiciário do Estado do Piauí - P.E. nº 04/2022;
q) Agência Nacional de Energia Elétrica - ANEEL - P.E. Nº 010/2022.

9. AVALIAÇÃO COMPARATIVA (BENCHMARKING)

9.1. Avaliando as características técnicas principais das soluções contidas no quadro acima, que são as soluções obtidas do quadrante “LEADERS” do Gartner, observamos que todas as soluções possuem características bem similares e atendem a maioria dos requisitos mínimos esperados na nova contratação.

9.2. Segue abaixo o quadro comparativo entre 3 soluções antivírus líderes no último relatório Gartner (2021). Selecionamos as características mais relevantes de um software “NG-AV” (Next-Generation Antivirus), tendo como base somente os fabricantes líderes. As informações são oriundas dos datasheets de cada solução, disponíveis nos websites oficiais dos respectivos fabricantes.

Tecnologia / Features	Sophos	Trend Micro	CrowdStrike
Centralized Management	Sim	Sim	Sim[1]
SaaS / Pure Cloud	Sim	Sim	Sim
On-Premise Management	Sim	Sim	Não[1]
Workstation Windows/Mac	Sim	Sim	Sim
Server Windows/Linux	Sim	Sim	Sim
Mobile IOS/Android	Sim	Sim	Sim
Exploit Prevention	Sim	Sim	Sim
Intensive Protection	Sim	Sim	Sim
Network Connection Security	Sim	Sim	Sim
Breach Assessment	Sim	Não[2]	Sim
Vulnerability Remediation	Sim	Sim	Sim
Application Isolation and Control	Sim	Sim	Sim
Device Control	Sim	Sim	Sim
Host Intrusion Prevention System	Sim	Sim	Não[2]
Firewall	Sim	Sim	Sim

Active Directory Security	Sim	Sim	Sim
Auto-Managed Policies	Sim	Sim	Sim
Targeted Attack Analytics	Sim	Sim	Sim
Behavioral	Sim	Sim	Sim
Threat Hunting	Sim	Sim	Sim
Web Control	Sim	Sim	Não[2]

[1] Painel de Gerenciamento centralizado na nuvem do fabricante.
[2] Não foram localizados em datasheets dos fabricantes.

10. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

10.1. Diante das opções concebidas durante os estudos técnicos que fundamentam o presente Termo de Referência, observadas as vantagens e desvantagens, técnicas e econômicas, optou-se, dentre 3 opções, pela solução 2 que, além de representar a melhor opção tecnológica para o atendimento do objeto, aparenta ser também a opção mais econômica para a contratação. Ademais, se mostrou mais viável para a contratação no contexto de um Sistema de Registro de Preços.

10.2. A solução 1 não implica custos diretos para os órgãos do Governo, mas oferece proteção bastante limitada, e ainda assim, apenas a um escopo limitado de dispositivos finais (sistemas Microsoft Windows) e, portanto, mostra-se inadequada ao atendimento da presente demanda.

10.3. Já o cenário 3 representa a escolha pela aquisição perpétua do licenciamento dos módulos EDR, por um período igual ao do cenário de subscrição. Considerando o modelo de negócio adotado pelos principais fabricantes das soluções, constatou-se que somente os módulos EDR estão disponíveis para aquisição perpétua, enquanto os demais itens somente via subscrição.

10.4. Assim, o objeto foi composto em lote único, contemplando as subscrições de licença de software (itens 1 ao 6), o serviço contínuo de detecção e resposta para a solução tecnológica (item 7), bem como os serviços de treinamento nas soluções (itens 8 ao 13).

11. DESCRIÇÃO DA SOLUÇÃO DE TIC COMO UM TODO

Contratação de empresa de Tecnologia da Informação para o fornecimento de solução de segurança para proteção de dispositivos finais (antivírus), aplicações em nuvem, servidores de e-mail e detecção/resposta unificada a eventos de segurança que envolvam a solução, contemplando o treinamento para operacionalização e o suporte técnico para as soluções contratadas.

12. JUSTIFICATIVA DO PARCELAMENTO DA SOLUÇÃO

12.1. Em que pese a distribuição do objeto por itens individuais, para fins de cotação e de contratação, faz-se necessário o agrupamento dos itens entre si, de forma a resguardar que os mesmos sejam oriundos de um mesmo fabricante, em razão de compatibilidade técnica, em resguardo do Enunciado nº 45 da Douta PGE-RJ, que diz:

> "*O objeto da contratação deve ser dividido em tantas parcelas quantas se comprovarem técnica e economicamente viáveis, priorizando-se a admissão da adjudicação por item e não por preço global, levando-se em consideração o melhor aproveitamento das potencialidades do mercado e a possível ampliação da competitividade do certame, sem perda de economia de escala, na forma dos arts. 15, inciso IV e 23, §1º da Lei n.º 8.666/93 e do art. 13, inciso IV, Decreto estadual n° 46.642 de 17 de abril de 2019.*"

12.2. O objeto é composto de itens distribuídos em um único lote. Os referidos itens podem ser contratados individualmente, com a possibilidade de integração da visibilidade, detecção, investigação e alertas de incidentes relativos aos componentes tecnológicos da solução.

12.3. Cada órgão participante da Ata de Registro de Preços, contratará os itens e respectivas quantidades, conforme a especificidade de sua estrutura, observado o Plano de Suprimentos (PLS) registrado para o certame.

12.4. O objeto ora pretendido se configura em uma solução de TI composta por mais de um item, onde determinados itens podem ser contratados individualmente (itens nº 01 ao nº 05), com a possibilidade de operação conjunta e unificada (mediante contratação dos itens nº 06 e/ou nº 07). Os demais itens do objeto (itens nº 08 ao nº 13) correspondem aos treinamentos para cada um dos componentes tecnológicos do objeto.

12.5. O agrupamento dos itens permite uma gestão mais eficiente do ambiente de TI, não apenas no âmbito da funcionalidade da solução, como também naquele relacionado à prevenção de contratações conflituosas e, por conseguinte, a resolução de conflitos entre fornecedores distintos. O modelo de contratação ora pretendido permite a preservação do funcionamento integrado, não comprometendo a funcionalidade de toda a solução, tendo em vista que o fornecimento, a instalação, a configuração, o suporte técnico e o treinamento serão executados por um único fornecedor representante do fabricante. Dessa forma, há uma redução do risco de perda, interrupção ou queda do funcionamento da solução e consequente indisponibilidade do serviço de TI, por conta de uma possível divisão de responsabilidades entre diferentes fornecedores.

12.6. Assim, entende-se que é fundamental para a pretensa contratação e para o alcance dos objetivos técnicos e estratégicos para os quais este projeto foi desenvolvido, que os itens componentes da solução tecnológica sejam contratados de forma agrupada.

12.7. Na situação em apreço, é imperativo destacar o que dispõe o Princípio da Padronização, consagrado na legislação licitatória pelo qual se estabelece que a Administração, sempre que possível, tem o objetivo de compatibilizar especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia, segundo transcrição a seguir, in verbis:

> "Lei nº 8.666/1993 Art. 15. As compras, sempre que possível, deverão:
>
> I - atender ao princípio da padronização, que imponha compatibilidade de especificações técnicas e de desempenho, observadas, quando for o caso, as condições de manutenção, assistência técnica e garantia oferecidas;
>
> (...);
>
> III - submeter-se às condições de aquisição e pagamento semelhantes às do setor privado;
>
> (...)"

12.8. Tal princípio visa a propiciar à Administração uma consecução mais econômica e vantajosa de seus fins; e serve, pois, como instrumento de racionalização da atividade administrativa, por meio da redução de custos financeiros, tecnológicos, operacionais, gerenciais, técnico-administrativos e da otimização da aplicação de recursos. Isto é, fatores que se coadunam e se verificam na contratação ora pretendida. Significa, portanto, que, nesse caso, a padronização elimina variações tanto no tocante à seleção de produtos no momento da contratação, como também na sua utilização, conservação, segurança e

manutenção.

12.9. Dividir o objeto entre fabricantes distintos, ocasionará prejuízos técnicos, como também riscos de danos tecnológicos, visto que o suporte técnico e o treinamento, se realizados por vários fornecedores, exigiriam um tempo excessivo em dirimir divergências entre possíveis incompatibilidades e causariam um potencial risco de operacionalização e funcionamento, pela adoção de procedimentos variados ou divergentes.

12.10. Justifica-se, portanto, o agrupamento dos itens da contratação com vista ao melhor aproveitamento das práticas de mercado adotadas pelos fabricantes da solução, resguardo da compatibilidade operacional da ferramenta, melhor gerenciamento do contrato e obtenção dos serviços de suporte e treinamento padronizados.

12.11. Conforme Acórdão nº 861/2013 - TCU - Plenário - é lícito os agrupamentos em lotes de itens a serem adquiridos por meio de pregão, desde que possuam mesma natureza e que guardem relação entre si. Além disso, a solução de TI, objeto da contratação em tela, embora possibilite a contratação dos itens em separado, resguarda a possibilidade do gerenciamento e operação unificada dos itens que compõem a solução tecnológica.

12.12. Segundo o Acórdão nº 5.260/2011 – TCU – 1ª câmara, de 06/07/2011, "Inexiste ilegalidade na realização de pregão com previsão de adjudicação por lotes, e não por itens, desde que os lotes sejam integrados por itens de uma mesma natureza e que guardem correlação entre si". O lote proposto nesse documento agrupa solução e serviços de uma mesma natureza, que guardam correlação entre si, seja por similaridade técnica ou de tecnologia, bem como de aplicabilidade em busca de uma única solução, sem causar qualquer prejuízo à competitividade.

12.13. O agrupamento também encontra amparo na jurisprudência do Tribunal de Contas da União, conforme se observa na Súmula 247 - TCU/2007. "É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade." (grifos nossos).

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

13. DA LICITAÇÃO

13.1. Natureza do objeto da contratação

13.1.1. Conforme descrito nos estudos técnicos preliminares, as atividades que integram o objeto da contratação possuem características comuns e usuais encontradas atualmente no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos no Termo de Referência. Portanto, se enquadram como SERVIÇOS COMUNS ou usuais de mercado.

13.1.2. O Objeto constitui solução em TIC em lote único, composto da seguinte forma:

a) Os itens nº 1 a 6 são serviços de subscrição de licença de software (locação / utilização de programa de informática), medidos em unidades;

b) O item nº 07 é medido em unidade e corresponde a serviço de prestação contínua;

c) Os itens nº 08 ao nº 13 são medidos por vaga/aluno e correspondem a serviços de treinamento.

13.1.3. Todos os itens serão demandados via emissão de Ordem de Serviço.

13.1.4. Sistema de Registro de Preços

13.1.5. Considerando as características do serviço que se pretende contratar e que os benefícios a serem alcançados com a presente contratação poderão beneficiar de forma significativa as demandas represadas dos órgãos da Administração Pública para o objeto a ser licitado, visando evitar a prestação descentralizada desse serviço, o que aumentaria significativamente seus custos, propõe-se a adoção do Sistema de Registro de Preços.

13.1.6. Além disso, as características do serviço, a potencial possibilidade de contratações frequentes e a impossibilidade de se estimar o quantitativo da demanda são argumentos que justificam a adoção da lógica do Sistema do Registro de Preços, entendimento que se extrai da legislação licitatória.

13.1.7. Em âmbito Estadual o tema é regulamentado pelo Decreto Estadual nº 46.751/2019. Nos termos do art. 3° do normativo referido "o Registro de Preços para a contratação de bens e serviços relativos a tecnologia da informação caberá ao Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro (PRODERJ), na qualidade de Órgão Gerenciador , conforme estabelecido pelo Decreto n° 46.665/2019."

13.1.8. Os serviços objeto do Registro de Preços poderão ser adquiridos pelo Órgão Gerenciador e pelos Órgãos e entidades da Administração Pública direta, autárquica e fundacional do Estado do Rio de Janeiro, ora denominados Órgãos Participantes.

13.1.9. A Ata de Registro de Preços poderá ser aderida por quaisquer órgãos ou entidades do Estado, que não tenham participado do certame licitatório, ora denominados Órgãos Aderentes.

13.1.10. Podem também ser considerados Órgãos Aderentes os órgãos ou entidades municipais, distritais, de outros estados e federais, resguardadas as disposições de cada ente.

13.1.11. O Órgão Aderente poderá, mediante prévia anuência do ÓRGÃO GERENCIADOR, aderir à Ata de Registro de Preços, desde que realizado estudo que demonstre a viabilidade e a economicidade.

13.1.12. O quantitativo decorrente da contratação pelos Órgãos Aderentes não ultrapassará, na totalidade, ao dobro de cada item da ata de registro de preços e nem poderá exceder, por Órgão Aderente, a cinquenta por cento do quantitativo de cada item desta licitação, registrados na Ata de Registro de Preços para o Órgão Gerenciador e Órgãos Participantes.

13.1.13. O Prazo de validade da Ata de registro de Preços será de 12 (doze) meses a contar da data da publicação de seu extrato no diário oficial.

13.1.14. A Ata de Registro de Preços poderá ser aderida durante a sua vigência por órgãos ou entidades do Estado que não tenham participado do certame licitatório, mediante anuência do PRODERJ, desde que realizado estudo que demonstre a viabilidade da economicidade.

13.2. Modalidade da licitação

13.2.1. O objeto da contratação foi conceituado pelo setor técnico responsável pelo planejamento da contratação nos estudos preliminares como "serviço de natureza comum" que segundo a legislação de regência são "identificados como aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, mediante as especificações usuais do mercado" (art. 1º, parágrafo único, da Lei nº 10.520/2002), vale dizer, bens de aquisição rotineira e habitual, cujas características encontrem no mercado padrões usuais de especificação, envolvendo critérios de julgamento rigorosamente objetivos, não havendo óbices a adoção do Pregão na modalidade eletrônica.

13.2.2. Desta forma, a modalidade de licitação mais adequada é o **PREGÃO**, nos termos do art. 1°, parágrafo único da Lei n° 10.520/2002 , sem nenhuma restrição de realização por **MEIO ELETRÔNICO**.

13.3. **Forma de adjudicação**

13.3.1. A forma de adjudicação do objeto será **MENOR PREÇO** global por lote.

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

14. JULGAMENTO DAS PROPOSTAS E CRITÉRIO DE ACEITAÇÃO DE PREÇOS

14.1. O critério de julgamento visará o menor preço global ofertado por lote.

14.2. A proposta de preços deverá ser feita em moeda nacional e englobará todas as despesas relativas ao objeto do contrato, bem como os respectivos custos diretos e indiretos, tributos, remunerações, despesas fiscais e financeiras e quaisquer outras necessárias ao cumprimento do objeto da Licitação, salvo expressa previsão legal. Nenhuma reivindicação adicional de pagamento de preços será considerada.

14.3. Demais considerações receberão tratativa no Edital.

15. CRITÉRIOS DE HABILITAÇÃO

15.1. **Qualificação Técnica**

15.1.1. Para fins de comprovação de qualificação técnica, deverão ser apresentados Atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem a experiência e aptidão de desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, referente às subscrições de software similares às pretendidas, que indiquem nome, função, endereço de contato do(s) atestador(es), ou qualquer outro meio para eventual contato pelo órgão licitante.

15.1.2. Um único atestado é suficiente para a demonstração da experiência anterior do licitante em relação a execução do objeto licitado, sendo possível o somatório de atestados de períodos concomitantes para comprovar a sua capacidade técnica.

15.1.3. O (s) atestado(s) deverão referenciar um quantitativo mínimo de 25% (vinte e cinco por cento) do volume estimado para os itens 1 e 2, cada, do lote único, uma vez que correspondem à parcela de maior relevância deste objeto.

15.1.4. Os percentuais exigidos se justificam em razão da necessidade da licitante classificada em primeiro lugar demonstrar que detém capacidade para executar simultaneamente os serviços, atendendo satisfatoriamente os quantitativos, em tempo hábil e atendendo ao volume e níveis de serviços.

15.1.5. Deverá acompanhar documentação indicando o modelo, marca e fabricante das soluções ofertadas, proposta técnica contendo a especificação clara e inequívoca de todos os itens.

15.1.6. Deverá acompanhar também declaração do licitante citada no subtópico 5.12.6 deste Termo de Referência

16. CRITÉRIOS DE ACEITAÇÃO DO OBJETO

16.1. O licitante deverá enviar, acompanhando os documentos de qualificação técnica tratados no tópico anterior, a documentação que informe o modelo, marca, fabricante da solução ofertada, bem como proposta técnica contendo a especificação clara e inequívoca de todos os itens, bem como o catálogo das soluções ofertadas pelo licitante.

16.2. **Teste de Bancada**

16.2.1. **Objetivo**

Será exigida do licitante classificado em primeiro lugar Teste de Bancada (Prova de Conceito) para a comprovação de que a solução ofertada é compatível com as exigências técnicas necessárias e prescritas para este objeto, conforme o roteiro apresentado no Anexo II deste Termo de Referência.

16.2.2. **Prazo e condições**

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

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

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

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

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

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

a) ID do requisito;

b) Descrição do requisito;

c) Nome do produto ofertado;

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

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

f) Outras informações necessárias.

16.2.2.3. Até o prazo de 5 dias úteis após a realização da reunião preparatória, será divulgada a equipe técnica que avaliará a solução durante o teste de bancada.

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

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

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

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

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

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

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

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

16.2.2.9. O teste de bancada será realizado entre 10:00 e 18:00 horas (horário de Brasília), com intervalo de 1 hora para almoço, e poderá durar de 1 a 5 dias úteis.

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

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

16.2.4. **Roteiro e critérios de avaliação**

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

16.2.4.2. Na sessão de teste de bancada, a equipe técnica do PRODERJ considerará apto o sistema que atender os requisitos conforme descrito no respectivo Roteiro para Teste de Bancada (Anexo II), do futuro Termo de Referência, onde cada item deverá ser preenchido, observados os critérios "atende" ou "não atende".

16.2.4.3. Durante o teste de bancada poderá ser feito questionamento, exclusivamente pelos representantes do PRODERJ à proponente permitindo a verificação dos requisitos estabelecidos.

16.2.4.4. Após a realização do teste de bancada será emitido e publicado o relatório descrevendo os testes realizados e a conclusão sobre a aprovação da proposta ou desclassificação bem como eventuais ocorrências ou manifestações de quaisquer dos presentes na sessão.

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

16.2.4.6. Será desclassificado a licitante que for convocada para o teste de bancada e não demonstrar a compatibilidade de seu produto conforme as especificações técnicas exigidas ou não comparecer no dia marcado sob qualquer pretexto.

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

16.2.5. **Responsabilidades**

16.2.5.1. Os custos para a demonstração da solução no teste de bancada são de responsabilidade do LICITANTE e em hipótese alguma caberá qualquer tipo de indenização.

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

16.2.5.3. A disponibilização de equipamentos, sistemas, demais materiais e/ou acessórios necessários ao ambiente de teste de bancada não informados pelo LICITANTE na reunião preparatória citada no subtópico 16.2.2.1 são de inteira responsabilidade do LICITANTE.

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

17. MODELO DE EXECUÇÃO DO CONTRATO

17.1. Horário de funcionamento do órgão é entre 09hs e 18hs, de segunda a sexta-feira, resguardadas eventuais emergências cuja ocorrência se dê em qualquer horário e dia.

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

17.3. **Condições de execução**

17.3.1. A execução será precedida de emissão de Ordem de serviço - OS, conforme modelo do Anexo III deste Termo de Referência.

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

17.3.3. A CONTRATADA deverá elaborar um Relatório de Cumprimento do Objeto sobre a prestação dos serviços, a ser entregue à Comissão de Fiscalização do Contrato quando da entrega do objeto, para a análise antes da emissão do Termo de Recebimento Provisório. O relatório deve contemplar todas as etapas e procedimentos realizados, eventuais problemas verificados e qualquer fato relevante sobre a execução do objeto contratual. O Relatório de

Cumprimento do Objeto deverá estar acompanhado, conforme item ou etapa entregue, das informações e/ou documentos conforme abaixo dispostos:

a) Para os serviços dos itens 1 a 6 do objeto: documentação que comprove o licenciamento das soluções contratadas, tais como número de séries, chaves, bem como dados informativos para o acionamento do suporte técnico/garantia e documentos oficiais do fabricante e documentação do produto e a disponibilização das soluções;

b) Para o serviço do item 7: relatórios mensais de segurança da informação abrangendo os ativos monitorados pelas soluções dos itens 1 a 6 e o relatório previsto no subtópico 19.23 deste documento;

c) Para os serviços dos itens 8 a 13 do objeto: certificados dos alunos treinados;

d) A CONTRATADA deverá entregar mensalmente, junto aos itens citados na alínea "b", os relatórios citados no subtópico 5.7.13 deste documento.

17.3.4. O cronograma (em dias úteis) para cumprimento do objeto é o seguinte:

Prazo	Marco para contagem do prazo	Atividades	Responsável
15	publicação do extrato do contrato no Diário Oficial (marco de vigência contratual)	Realização da Reunião Kick Off prevista no subtópico 5.6.1.1.	Contratante e Contratada
5	reunião kick off	Liberação do acesso da Contratante na plataforma SaaS de gerenciamento da solução, onde deverá constar a totalidade das licenças contratadas.	Contratada
20	emissão da Ordem de Serviço	Treinamento na solução	Contratada
15	reunião kick off	Instalação dos agentes da solução nos ativos tecnológicos que foram indicados pela Contratante na reunião de “kick-off”.	Contratada
30	reunião kick off	Conclusão da implementação da configuração inicial básica da solução (entrega definitiva)	Contratada
1	Conclusão da implementação da configuração inicial básica da solução	Início da prestação do serviço do item 7 (quando contratado)	Contratada
2	Recebimento do Relatório de Cumprimento do Objeto, previsto no subtópico 17.3.3.	Recebimento provisório	Contratante
20	Emissão do Termo de Recebimento Provisório	Emissão do Termo de Recebimento Definitivo / autorização para emissão de Nota Fiscal ou fatura.	Contratante

17.3.5. **Transferência de conhecimento, tecnologia e técnicas empregadas e transição contratual**

17.3.5.1. Ao final do contrato, a Contratada deverá promover a transição contratual com vistas a não impactar a rotina do órgão contratante;

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

17.4. **Mecanismos de comunicação a serem estabelecidos**

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

a) Ordens de Serviço;

b) Plano de Inserção;

c) Termos de Recebimento;

d) Chamado registrado na Central de Atendimento;

e) Ofícios;

f) Relatórios e Atas de Reunião;

g) E-mail;

h) Demais Termos previstos no instrumento convocatório.

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

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

17.5. **Forma, local, prazo de entrega e endereço de entrega**

17.5.1. Os serviços devem ser executados preferencialmente nos horários de 09h às 18hs. Apesar dos horários preferenciais de execução, os suportes técnicos que compõem essa contratação devem respeitar os requisitos de disponibilidade dos Serviços de TI fornecidos aos usuários da CONTRATANTE. Qualquer atividade que possa ocasionar indisponibilidade deve ser preferencialmente executada após as 22:00 horas em dias de semana; nos finais de semana e feriados, ou a critério da CONTRATANTE.

17.5.2. Os serviços serão executados nas modalidades remota e presencial, de acordo com as definições da CONTRATANTE a serem estabelecidas em reuniões preparatórias ou na Ordem de Serviço.

17.5.3. Os locais de entrega constam da tabela do subtópico 6.3 ou conforme indicado pela CONTRATANTE, considerada a hipótese de entrega em modalidade virtual em comum acordo entre CONTRATANTE e CONTRATADA.

17.5.4. Os prazos e local/modalidade de execução constarão em cada Ordem de Serviço estabelecida.

17.5.5. O objeto em sua totalidade é composto de subscrições de software, com um serviço de monitoramento, alertas e relatoria, mais os respectivos cursos de treinamentos nos módulos da solução. A entrega dos itens 1 a 6 do objeto se dará de forma virtual, via liberação do acesso na plataforma da solução onde constará o total de licenças contratadas. Para fins de entrega do objeto, a prestação do serviço contínuo referente ao item 7 está condicionada à entrega definitiva das subscrições dos itens 1 a 6. A execução dos itens 8 a 13 do objeto (cursos de treinamento) acontecerá através do portal de treinamentos da empresa contratada ou que esta venha a viabilizar.

18. FISCALIZAÇÃO DO CONTRATO

A execução do contrato será acompanhada e fiscalizada por comissão de fiscalização de contrato composta por 3 (três) membros da Contratante, especialmente designados pela autoridade competente.

19. ACORDO DE NÍVEL DE SERVIÇO

19.1. **Finalidade:** Garantir a qualidade do Serviço gerenciado de detecção e resposta - MDR (item 07 do lote), bem como do Suporte Técnico dos itens 01 a 06 (subscrições de licenças de software.

19.2. **Periodicidade**: Mensal.

19.3. **Início da medição:** A partir do 2º mês após a plena instalação e configuração da solução tecnológica (itens nº 01 ao nº 06).

19.4. **Mecanismo de cálculo**: Somatório dos índices correspondentes aos eventos previstos nas alíneas "a, b, c, d, e" do subtópico 33.1 deste Termo de Referência, verificados durante o período.

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

Níveis de severidade dos chamados			
Categoria	**Descrição**	**Tempo de Resposta**	**Tempo de Solução**
Urgente	Risco iminente de comprometimento do ativo	até 1 hora	até 4 horas
Crítico	Capacidade de resposta limitada por anomalias nas tecnologias de proteção	até 2 horas	até 8 horas
Alerta	Serviço com degradação de performance ou funcionalidade em sua capacidade de mitigar riscos e detectar exploração de ataques	até 3 horas	até 12 horas

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

19.7. A severidade do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução.

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

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

19.10. O descumprimento deste acordo de nível de serviço, notadamente quanto ao cumprimento dos prazos, ensejará as sanções previstas no tópico 33 deste Termo de Referência.

19.11. A Contratada deverá prover monitoramento, telemetria, atividades proativas de Threat hunting e times de detecção e resposta em regime de 24x7 (vinte e quatro horas por dia, sete dias por semana);

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

19.13. Tempo de resposta: Os atendimentos deverão ser respondidos e classificados em um prazo compatível com o nível de urgência especificado no momento da abertura do chamado ou identificação da anomalia e iminência de exploração, conforme descrito na tabela do subtópico 19.5.

19.14. Tempo de solução: o tempo de solução de problemas dependerá de sua extensão, gravidade, disponibilidade e risco a disponibilidade ou integridade aos ativos da instituição. A CONTRATADA deverá fornecer uma estimativa de tempo para solução do problema dentro da primeira hora de atendimento. O tempo já não está estabelecido na tabela 19.5?

19.15. Os prazos de atendimento poderão ser prorrogados, desde que aceitas as justificativas apresentadas pela CONTRATADA que revelem a necessidade de dilatação do prazo.

19.16. Atendimento no local: Nos casos classificados como grau de severidade urgente, quando a intervenção remota não for efetiva, após decorrido o prazo da estimativa de tempo fornecido para a solução do problema, a CONTRATADA deverá, imediatamente e às suas custas, deslocar um técnico com o perfil necessário para atender ao problema em no máximo até 24 (vinte e quatro horas).

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

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

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

19.20. A Comissão de Fiscalização do Contrato deverá comunicar mensalmente à Contratada, o resultado da apuração até o segundo dia útil do mês subsequente.

19.21. A comunicação poderá ser feita pessoalmente, ou por meio eletrônico. As ocorrências apuradas no mês serão aplicadas no período seguinte.

19.22. Cada Nota Fiscal deverá ser encaminhada pela Comissão de Fiscalização do Contrato ao seu Setor Financeiro juntamente com o descritivo de ocorrências.

19.23. A CONTRATADA deverá enviar mensalmente relatório resumido dos atendimentos realizados no período.

20. OBRIGAÇÕES DA CONTRATANTE

a) Realizar os pagamentos devidos à contratada, nas condições estabelecidas;

b) Fornecer à Contratada documentos, informações e demais elementos que possuir pertinentes à execução dos serviços;

c) Exercer a fiscalização do contrato conforme níveis de serviços estabelecidos;

d) Receber provisória e definitivamente o objeto do contrato, nas formas definidas no edital e no contrato;

e) Encaminhar formalmente a demanda por meio de Ordem de Serviço, de acordo com os critérios estabelecidos no Termo de Referência;

f) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável; e

g) Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável.

21. OBRIGAÇÕES DA CONTRATADA

a) Conduzir os serviços de acordo com as especificações técnicas e níveis de serviços estabelecidos;

b) Prestar os serviços nos endereços indicados;

c) Prover os serviços ora contratados nos prazos estipulados;

d) Comunicar ao Fiscal do contrato, por escrito e tão logo constatado problema ou a impossibilidade de execução de qualquer obrigação firmada, para a adoção das providências cabíveis;

e) Reparar, corrigir, remover, reconstruir ou substituir, no todo ou em parte e às suas expensas, bens ou prestações objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de execução irregular ou do emprego ou fornecimento de materiais inadequados ou desconformes com as especificações deste Termo de Referência;

f) Manter-se durante toda a prestação do serviço sem compatibilidade com as obrigações assumidas, as condições de habilitação e qualificação exigidas.

g) Indenizar todo e qualquer dano e prejuízo pessoal ou material que possa advir, direta ou indiretamente, do exercício de suas atividades ou serem causados por seus prepostos à Contratante, aos usuários ou terceiros;

h) Fornecer, sem custos adicionais para a Contratante, quaisquer materiais e/ou acessórios, previstos e não previstos, necessários ao pleno funcionamento da solução contratada, assim como dos treinamentos;

i) Disponibilizar ambiente web, número de telefone ou e-mail para abertura de chamados e acompanhamento das soluções e esclarecimentos de dúvidas;

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

k) Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

l) Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE;

m)Manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;

n) Manter total sigilo e confidencialidade, por si, por seus empregados ou representantes, no que se refere a não divulgação, por qualquer forma ou meio, de toda ou parte de informações ou documentos sobre a Contratante, ou sob guarda da Contratante, bem como toda a informação a respeito dos negócios, ideias, produtos, clientes ou serviços, às quais venha a ter acesso, em decorrência da prestação dos serviços executados;

o) Responsabilizar-se em caso de quebra de sigilo ou mau uso das informações obtidas por seus funcionários ou representantes, em razão da prestação dos serviços;

p) Respeitar integralmente as normas de segurança estabelecidas pela CONTRATANTE, atendendo os padrões de segurança e controle para acesso e uso das instalações e equipamentos, zelando por sua integridade;

q) Disponibilizar previamente as informações necessárias para acesso aos ambientes físico lógico da CONTRATANTE, para que a mesma analise a liberação dos acessos às dependências, de funcionários, equipamentos, softwares e sistemas que forem necessários ao cumprimento do objeto;

r) Realizar, no fim do contrato, a transição contratual, a saber: a transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações à CONTRATANTE;

s) Arcar com as despesas e responsabilidade pela obtenção das autorizações quanto às eventuais permissões, aprovações e/ou licenças, bem como as respectivas eventuais renovações, junto das autoridades governamentais federais, estaduais e municipais, agentes do serviço público, concessionárias de serviços públicos e quaisquer outros Órgãos/Entidades que se façam necessários à execução do objeto, durante todo o prazo da contratação.

21.1. A CONTRATADA deverá assinar um termo de confidencialidade e sigilo, na forma do modelo do anexo IV deste documento, a ser anexado ao contrato principal.

22. CRITÉRIOS DE RECEBIMENTO E ACEITAÇÃO DO OBJETO

22.1. O objeto será recebido em tantas parcelas quantas forem a do pagamento, da seguinte forma:

a) provisoriamente, após parecer circunstanciado, que deverá ser elaborado pela Comissão de Fiscalização no prazo de 02 (dois) após a entrega do serviço e do Relatório de Cumprimento do Objeto previsto no subtópico 17.3.3. deste documento;

b) definitivamente, mediante parecer circunstanciado da comissão de fiscalização, após decorrido o prazo de 20 (vinte) dias a contar do recebimento provisório, para observação e vistoria, que comprove o exato cumprimento das obrigações contratuais.

22.2. O fornecedor deverá entregar à Comissão de Fiscalização do Contrato, o Relatório de Cumprimento do Objeto e documentos anexos, disposto no subtópico 17.3.3 e alíneas "a, b, c, d", quando da entrega do objeto, para a devida análise e para fins de emissão do Termo de Recebimento Provisório.

22.3. O ato de cumprimento do serviço será marcado pela entrega, por parte da CONTRATADA, do acima referido Relatório de Cumprimento do Objeto, bem como os demais documentos comprobatórios, conforme o item entregue.

22.4. A CONTRATANTE analisará a documentação entregue e poderá fazer inspeção quanto às etapas executadas para entrega do objeto, por meio de sua equipe técnica, com a finalidade de verificar a adequação no cumprimento do objeto pela contratada para fins de constatar e relacionar os arremates, retoques e revisões finais que eventualmente se fizerem necessários.

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

22.6. O prazo para a emissão do recebimento definitivo contará a partir da emissão do recebimento provisório, resguardadas eventuais compensações para fins de eventuais ajustes.

22.7. Com o recebimento definitivo, que concretiza o ateste do cumprimento do objeto contratado, a CONTRATANTE comunicará à CONTRATADA para que, em até 5 dias, emita a Nota Fiscal ou Fatura, com o valor exato dimensionado na respectiva Ordem de Serviço.

23. FORMA DE PAGAMENTO

23.1. **Forma de pagamento**

23.1.1. À vista, sob demanda, para os itens nº 01 ao nº 06 do lote, correspondentes aos serviços de subscrições de licenças de software, observada a emissão de Termo de Recebimento Definitivo pela Comissão Fiscal do Contrato.

23.1.2. parcelado e mensal para o item nº 07 do lote, correspondente ao serviço de gerenciamento centralizado, a começar após a entrega definitiva dos itens nº 01 ao nº 06.

23.1.3. à vista, sob demanda, para os itens nº 08 ao nº 13 do lote, correspondentes aos serviços de treinamento, observada a emissão de Termo de Recebimento Definitivo pela Comissão Fiscal do Contrato.

23.2. **Prazo do pagamento**

23.2.1. O prazo de pagamento será de até 30 (trinta) dias, a contar da data final do período de adimplemento de cada parcela.

23.2.2. Considera-se adimplemento o cumprimento da prestação com a entrega do objeto, devidamente atestada pelo(s) agente(s) competente(s).

23.3. **Periodicidade do pagamento**

23.3.1. Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível ao CONTRATADO, sofrerão a incidência de atualização financeira pelo IBGE/IPCA, e juros moratórios de 0,5% ao mês, calculado *pro rata die,* e aqueles pagos em prazo inferior ao estabelecido neste Edital serão feitos mediante desconto de 0,5% ao mês *pro rata die.*

23.3.2. As demais condições de pagamento constam do Edital.

24. VIGÊNCIA CONTRATUAL

24.1. O prazo de vigência do contrato será de 36 (trinta e seis) meses, contados a partir de publicação do extrato de seu instrumento no D.O.

24.2. O prazo contratual poderá ser prorrogado, observando-se o limite de até 48 (quarenta e oito) meses, observado o Enunciado nº 46 da Douta Procuradoria-Geral do Estado do Rio de Janeiro, desde que a proposta da Contratada **seja mais vantajosa para o Contratante**.

25. REAJUSTE DE PREÇOS

25.1. Os valores constantes da Ata de Registro de Preços não sofrerão reajuste, exceto nos casos previstos nos art. 21 e art. 22, do Decreto Estadual nº 46.751/2019, para a renegociação de preços junto aos fornecedores registrados, nos casos em que os preços praticados na Ata de Registro de Preços se tornarem superiores aos preços de mercado, resguardadas as disposições do Edital.

25.2. Os contratos poderão ter os seus preços reajustados, observado o interregno mínimo de 12 (doze) meses contados da data limite da apresentação da proposta pela empresa contratada, aplicando-se a variação do Índice de Custo da Tecnologia da Informação – ICTI, ou outro que o venha substituir.

25.3. O Reajustamento ocorrerá na forma da legislação licitatória.

26. GARANTIA CONTRATUAL

26.1. Exigir-se-á do fornecedor, no prazo máximo de 10 (dez) dias, contado da data da assinatura do contrato, comprovante de prestação de garantia da ordem de 5% (cinco por cento) do valor do contrato, a ser prestada em qualquer modalidade prevista no §1º, do art. 56 da Lei n.º 8.666/93, a ser restituída após sua execução satisfatória.

26.2. O referido percentual, resguardada a discricionariedade prevista no art. 56, caput, da Lei nº 8.666/93 e o teto estabelecido no seu §2º, considera a natureza do objeto, enquanto ferramenta estratégica de caráter tecnológico de relevância para as atividades do órgão contratante em razão das exigências trazidas pela nova legislação quanto ao tratamento de dados pessoais.

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

a) Prejuízos advindos do não cumprimento do contrato;

b) Multas punitivas aplicadas pela fiscalização à contratada;

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

d) Obrigações previdenciárias e trabalhistas não honradas pela Contratada.

26.4. Caso o valor do contrato seja alterado, de acordo com o art. 65 da Lei Federal n.º 8.666/93, a garantia deverá ser complementada, no prazo de 72 horas, para que seja mantido o percentual de 5 % do valor do Contrato.

26.5. Nos casos em que valores de multa venham a ser descontados da garantia, seu valor original será recomposto no prazo de 72 horas, sob pena de rescisão administrativa do contrato.

27. CRITÉRIOS E PRÁTICAS DE SUSTENTABILIDADE

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

28. SUBCONTRATAÇÃO

Não se aplica a subcontratação em razão da natureza do objeto, enquanto serviço em lote único para fornecimento de solução integrada e que implica subordinação.

29. POSSIBILIDADE DE PARTICIPAÇÃO EM CONSÓRCIO

29.1. Não será permitida a participação em regime de consórcio.

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

30. POSSIBILIDADE DE PARTICIPAÇÃO DE COOPERATIVA

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

30.2. Diante da especificidade desta contratação, que trata do fornecimento, por subscrição, de licenças de software, bem como o respectivo sistema de gerenciamento e respectivos cursos de treinamento, englobados em lote único, bem como observado o mercado de soluções para o objeto ora proposto, composto por empresas de organização tradicional aptas a fornecer a integralidade do objeto, não se faz razoável a participação de cooperativas neste certame.

30.3. Saliente-se que os serviços estimados no presente documento requerem conhecimento técnico especializado nas soluções aplicadas, além do fornecimento de licença de software, equipamentos, serviços de garantia e suporte técnico e treinamento, não havendo no mercado cooperativa capaz de atender aos requisitos e padrões técnicos exigidos.

31. CONTRATAÇÕES CORRELATAS OU INTERDEPENDENTES

Este Termo de Referência trata de mesmo objeto no âmbito do SEI-150016/000074/2022: "O presente Contrato tem por objeto a prestação de serviços de subscrição de licenças de software para solução Antivírus, incluindo console de gerenciamento, suporte, instalação, treinamento, garantia e atualização irrestrita para a última versão existente do fabricante por 36 meses, na forma do Termo de Referência e do instrumento convocatório."

32. ESTRATÉGIA DE INDEPENDÊNCIA EM RELAÇÃO À CONTRATADA

32.1. Para os itens 1 até 6: Por se tratar da contratação de serviço de subscrição/licenciamento de uso de softwares do fabricante, o pagamento integral das licenças garante, pelo fabricante, a utilização dos produtos por 36 meses, com suporte do mesmo pelo fabricante já incluso no licenciamento, sem risco de rescisão ou interrupção antecipada no funcionamento dos produtos. Portanto, não se aplica a existência de um plano de sustentação.

32.2. Para o Item 7: Serviço gerenciado de detecção e resposta – MDR, em caso de interrupção contratual, as atividades relativas a este serviço teriam de ser emergencialmente executadas pela Contratante até a realização de nova contratação, ou seja, a equipe da Contratante deverá operar e mitigar todos os alertas e eventos de segurança das soluções tecnológicas que constituem o objeto. Saliente-se que este item corresponde a serviço opcional.

32.3. Os itens 8 até 13: são os serviços de treinamento na solução, cujo pagamento é efetuado após sua realização, sem risco de interrupção do serviço. Logo, não há necessidade de um plano de sustentação.

33. SANÇÕES

33.1. Ocorrerá aplicação de glosas/multas por motivo de descumprimento do Acordo de Nível de Serviços previsto no tópico 19 deste Termo de Referência, conforme os valores a seguir:

a) 0,15% no valor da fatura do item correspondente do mês de referência, por demanda categorizada como “alerta” ou "normal" não atendida;

b) 0,25% no valor da fatura do item correspondente do mês de referência, por demanda categorizada como “crítico” não atendida;

c) 0,50% no valor da fatura do item correspondente do mês de referência, por demanda categorizada como “urgente” não atendida. Esta penalidade poderá ser mitigada, se o problema for solucionado nos termos do subtópico 19.16 deste Termo de Referência;

d) 2% no valor da fatura do item correspondente do mês de referência, por hora de indisponibilidade total, após o vencimento do prazo indicado na tabela;

e) 1% no valor da fatura do item correspondente do mês de referência, por hora de indisponibilidade parcial, após o vencimento do prazo indicado na tabela.

33.2. Os descontos relativos à redução por não cumprimento do nível de serviço, referente ao item 7, serão aplicados nas faturas dos meses subsequentes, resguardada a ampla defesa e contraditório;

33.3. Os descontos relativos à redução por não cumprimento do nível de serviço não serão aplicados para demandas não rotineiras, no caso, por

exemplo, de novas instalações;

33.4. Qualquer descumprimento do nível de serviço mínimo exigido poderá implicar a aplicação da legislação licitatória quanto à inexecução e à rescisão dos contratos;

33.5. Ficam resguardadas as demais sanções previstas em lei conforme o Edital.

34. ANEXOS

I - Especificações Técnicas do Objeto (63878350);

II - Roteiro para Teste de Bancada (63879925);

III - Modelo de Ordem de Serviço (63879694);

IV - Modelo de Termo de Confidencialidade e Sigilo (63879241);

V - Modelo de Planilha de Composição de Lances (63880427).

35. ASSINATURA DOS RESPONSÁVEIS PELA ELABORAÇÃO

Fabio Ivo Analista de Rede/Telecom ID 5143032-0	Manuelito de Sousa Reis Júnior Gerente de Riscos e Ameaças ID 4406953-7

Rio de Janeiro, 23 de novembro de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/11/2023, às 11:04, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 24/11/2023, às 11:19, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **63876832** e o código CRC **2837F8CE**.

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

Governo do Estado do Rio de Janeiro

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

Diretoria de Segurança da Informação

ANEXO I DO TERMO DE REFERÊNCIA

ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1. OBJETO

O lote com os itens componentes do objeto se encontra descrito na tabela do subtópico 6.2 do Termo de Referência.

2. CARACTERÍSTICAS E FUNCIONALIDADES GERAIS DAS SOLUÇÕES

2.1. Instalação e Configuração

As especificações de instalação e configuração da solução, abrangendo os itens 1, 2, 3, 4, 5, 6 e 7 encontram-se no subtópico 5.6.1. do Termo de Referência.

2.2. Suporte Técnico

As especificações do Suporte Técnico da solução, abrangendo os itens 1, 2, 3, 4, 5, e 6 encontram-se no subtópico 5.7. do Termo de Referência.

2.3. Características gerais da solução tecnológica (itens 1, 2, 3, 4, 5 e 6)

2.3.1. Identificar e eliminar a maior quantidade possível de ameaças cibernéticas;

2.3.2. O EDR deve analisar arquivos, execuções de memória e tráfego de rede dos endpoints; verificar continuamente os discos rígidos (HD's) e demais mídias de armazenamento de forma transparente ao usuário;

2.3.3. Identificar e proteger contra as várias vulnerabilidades dos sistemas operacionais e aplicações dos endpoints;

2.3.4. A solução deve permitir a atualização centralizada, automática ou programada, dos componentes da solução e da base de ameaças cibernéticas. Estas atualizações deverão ser realizadas de maneira criptografada (SSL/TLS);

2.3.5. Fornecer visibilidade das ameaças do parque tecnológico da Contratante;

2.3.6. Proteger os endpoints contra os ataques de criptografia (ransomware);

2.3.7. O conjunto de softwares que compõe a solução de EDR para estações de trabalho, dispositivos móveis e servidores deverá ser do mesmo fabricante, deverá ainda ser compatível com a solução XDR, disponível no Lote Único, de modo a permitir a integração e correlação de eventos de segurança dos endpoints;

2.3.8. O fabricante da solução deve dispor de laboratório próprio para desenvolvimento de vacinas e engines. Esta informação deve ser comprovada pelo Fabricante através de documentação oficial;

2.3.9. A solução deverá possuir filtro de reputação de websites e arquivos, ferramentas de

varredura, detecção, análise e remoção de malware e riskware e demais formas de vírus e códigos maliciosos conhecidos, ameaças desconhecidas e ataques do tipo fileless (malware sem arquivo);

2.3.10. Os itens 1, 2, 3, 4, e 5 do Objeto, correspondentes às licenças de uso da solução EDR (Desktops, servidores e mobile), proteção de apps em nuvem e proteção a servidores de e-mail, devem possuir painéis de gerenciamento específicos para cada módulo, viabilizando a contratação individual dos referidos itens;

2.3.11. A solução, através do painel/GUI unificado dos itens 6 e 7, deverá possibilitar a centralização da visibilidade, detecção, investigação e resposta a incidentes em ativos tecnológicos que estejam dentro do escopo de licenciamento dos itens 1, 2, 3, 4 e 5 do objeto. O acesso autenticado a esta interface centralizada deverá ser feito via navegador (ao menos: Chrome, Firefox e Edge em suas versões atuais) com HTTPS. Alternativamente, o acesso poderá ser feito via cliente no Windows.

2.3.12. A solução ofertada deverá dispor de uma base de conhecimento e documentação da ferramenta em um portal com acesso público;

2.3.13. As consoles de administração deverão permitir o envio de notificações via SMTP;

2.3.14. Todos os eventos e ações realizadas nas consoles de gerenciamento precisam ser gravados para fins de auditoria;

2.3.15. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

2.3.16. A solução deverá permitir a criação de dashboards configuráveis, para facilitar a administração e visualização dos eventos;

2.3.17. A solução deve permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob demanda, ou agendado, incluindo ao menos os formatos: PDF, CSV e XLS, com o envio automático do relatório via e-mail;

2.3.18. A solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

2.3.19. A solução deve ter a capacidade de conceder determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

2.3.20. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

2.3.21. Para efeito de administração, a solução deverá avisar quando um agente se encontrar desconectado da sua console de gerenciamento;

2.3.22. A solução deve permitir a configuração do período para remoção automática de agentes inativos;

2.3.23. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

2.3.24. A solução deverá mostrar quais hosts estão usando determinada política;

2.3.25. A solução deverá ter a capacidade de enviar logs para soluções de SYSLOG e SIEM de terceiros;

2.3.26. As consoles de gerenciamento devem ter a capacidade de realizar o roll back de suas atualizações de regras;

2.3.27. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

2.3.28. A solução deve mostrar a quantidade de licenças contratadas e a quantidade delas que estão em uso;

2.3.29. A solução deverá ter a capacidade de classificar eventos, de modo a facilitar a identificação e visualização de eventos críticos;

2.3.30. No que diz respeito aos módulos da solução que atuam em sistemas Microsoft Windows, o fabricante deverá ser membro do programa “Microsoft Active Protection Program”, de modo que a solução tenha acesso prévio a patches e correções daquele fabricante;

2.3.31. A solução deve possuir API documentada para integração na esteira de automação;

2.3.32. O administrador da solução poderá desabilitar funcionalidades específicas dos módulos EDR.

2.3.33. A Contratante fornecerá a política de segurança cibernética organizacional estabelecida de forma que a Contratada reflita as orientações nos serviços prestados.

3. DETALHAMENTO DOS ITENS DO OBJETO

3.1. Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para estações de trabalho, Incluídos instalação, configuração e suporte por 36 meses (item 1)

3.1.1. A solução deve atender os seguintes sistemas operacionais:

3.1.1.1. Windows 8.1 (32/64-bit);

3.1.1.2. Windows 10 (32/64-bit);

3.1.1.3. Windows 11 (64-bit);

3.1.1.4. mac OS 10.14 e superiores.

3.1.2. Funcionalidade de Administração e Gerência

3.1.2.1. A solução Antivírus_EDR do item 1 deverá ser gerenciada através de painel centralizado, disponibilizado na nuvem da Contratada ou do Fabricante da Solução, onde o acesso ocorrerá de maneira criptografada (SSL/TLS). Alternativamente, este painel poderá ser posicionado dentro da infraestrutura da Contratante, que será então responsável pelos equipamentos físicos ou virtuais onde o componente será instalado. No caso de gerenciamento on premise, a console/ painel deverá ser compatível com Windows Server 2016 e superiores;

3.1.2.2. Na alternativa on premise, a solução deve suportar base de dados Microsoft SQL Server;

3.1.2.3. A console de gerenciamento centralizado deve permitir a integração e correlação de eventos entre todos os componentes da solução ofertada;

3.1.2.4. A solução deve gerenciar logs das atividades e eventos gerados pela solução;

3.1.2.5. Nas informações da política, devem constar ao menos os seguintes dados: nome, status, dono da política, horário e data da última alteração;

3.1.2.6. A gerência central deverá mostrar quais estações estão sem políticas;

3.1.2.7. A Solução deve gerar relatório de compliance com informações de máquinas que nunca realizaram scan, políticas inconsistentes entre servidor/agente e componentes desatualizados;

3.1.2.8. A solução deve possuir integração com Microsoft Active Directory;

3.1.2.9. A solução deve permitir níveis de administração da console por usuários ou grupos de usuários;

3.1.2.10. A solução deve permitir a constituição de políticas genéricas aplicáveis a máquinas, grupos de usuários ou máquinas;

3.1.2.11. A solução deve disponibilizar sua interface através dos protocolos http e https;

3.1.2.12. A solução deverá gerar relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

3.1.2.13. A solução deverá gerar relatórios e gráficos pré-definidos nos formatos pdf, docx e xlsx;

3.1.2.14. Os relatórios devem conter informações de efetividade, ransomware, canais de infecção, principais usuários que receberam ameaças, vírus e spyware;

3.1.2.15. A solução deve permitir criação de modelos de relatórios customizados;

3.1.2.16. A solução deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

3.1.2.17. A solução deve permitir o controle individual de cada componente a ser atualizado;

3.1.2.18. A solução deve permitir a definição de exceções por dias e horas para não realização de atualizações;

3.1.2.19. A solução deve permitir ter como fonte de atualização um compartilhamento de rede em pelo menos um dos seguintes formatos: UNC, NFS e SMB;

3.1.2.20. A solução deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

3.1.2.21. A solução deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

3.1.2.22. A solução deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

3.1.2.23. Deve permitir a configuração do intervalo de comunicação com os módulos gerenciados;

3.1.2.24. Deve permitir a escolha do intervalo de tempo necessário para que uma estação seja considerada off-line;

3.1.2.25. Deve possuir a configuração do tempo de expiração da sessão dos usuários;

3.1.2.26. Deve permitir a configuração do número de tentativas inválidas de login para o bloqueio de usuários;

3.1.2.27. Deve possuir templates de acesso a console de gerenciamento;

3.1.2.28. Deve permitir a configuração da duração do bloqueio;

3.1.2.29. Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;

3.1.2.30. Deve permitir pesquisas personalizadas para a consulta de eventos (logs), através de critérios lógicos, com base em todos os campos pertencentes aos eventos consultados;

3.1.2.31. Deve permitir a configuração da manutenção dos registros de eventos (logs), com base no intervalo de tempo que devem ser mantidos e no número máximo de registros, por tipo de evento;

3.1.2.32. Deve de permitir a criação de políticas de segurança personalizadas;

3.1.2.33. Deve permitir visualização de eventos de violação de segurança de todos os módulos gerenciados, agrupado por usuário numa linha de tempo, configurável;

3.1.2.34. Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;

3.1.2.35. A solução deverá possuir um dashboard pré-configurado com informações sobre estações desatualizadas, usuários afetados, estações sem o antimalware instalado, estações afetadas e ameaças críticas tipo Ransomware, ameaças desconhecidas, vulnerabilidades e vazamento de dados;

3.1.2.36. Os blocos de informações pertencentes aos painéis personalizáveis devem permitir filtros personalizados para facilitar na visualização e gerenciamento;

3.1.2.37. A seleção de uma informação específica dentro de um bloco de informações, através de um clique, deve redirecionar ao log detalhado que gerou aquela informação;

3.1.2.38. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada

pela console de administração da solução completa;

3.1.2.39. Deve possibilitar instalação "silenciosa";

3.1.2.40. Deve permitir o travamento de pastas e diretórios compartilhados;

3.1.2.41. Deve permitir o travamento de portas de comunicação;

3.1.2.42. Deve permitir o rastreamento e bloqueio de infecções;

3.1.2.43. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

3.1.2.44. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

3.1.2.45. Deve permitir a desinstalação através da console de gerenciamento da solução;

3.1.2.46. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

3.1.2.47. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

3.1.2.48. Deve permitir a deleção dos arquivos quarentenados;

3.1.2.49. Deve permitir remoção automática da exibição na console de clientes inativos por determinado período de tempo;

3.1.2.50. Deve permitir integração com Active Directory para acesso a console de administração;

3.1.2.51. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução instalada;

3.1.2.52. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;

3.1.2.53. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;

3.1.2.54. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

3.1.2.55. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

3.1.2.56. Deve registrar no sistema de monitoração de eventos da console da solução, informações relativas ao usuário logado no sistema operacional;

3.1.2.57. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console da solução e não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;

3.1.2.58. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

3.1.2.59. Deve permitir a criação de usuários locais de administração da console;

3.1.2.60. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

3.1.2.61. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;

3.1.2.62. Deve ser capaz de enviar eventos aos respectivos administradores de cada domínio definido na console de administração;

3.1.2.63. Deve permitir a programação de atualizações automáticas das listas de definições

de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

3.1.2.64. Deve permitir atualização incremental da lista de definições de vírus;

3.1.2.65. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

3.1.2.66. Deve permitir o rollback das atualizações das listas de definições de vírus e engines.

3.1.3. Características de proteção a endpoints

3.1.3.1. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações, Controle de dispositivos e EDR (Endpoint Detection and Response) em um único agente.

3.1.3.2. Funcionalidade Anti-Malware

3.1.3.2.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

3.1.3.2.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

3.1.3.2.3. A solução deve possuir listas de exclusão separadas por funcionalidade da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

3.1.3.2.4. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção.

3.1.3.2.5. Em endpoints Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

3.1.3.2.6. A solução deverá ter a capacidade de monitorar o comportamento do sistema, de modo a detectar mudanças e atividades suspeitas não autorizadas;

3.1.3.2.7. A solução deverá ser capaz de escanear processos em memória, a fim de detectar Malwares;

3.1.3.2.8. Deverá ser possível configurar os níveis de camadas de compressão para a varredura de arquivos comprimidos;

3.1.3.2.9. Deverá realizar varredura de arquivos comprimidos do tipo OLE, sendo possível configurar as camadas de compressão;

3.1.3.2.10. A solução deve permitir iniciar ou cancelar escaneamento manual a partir de uma notificação recebida no endpoint;

3.1.3.2.11. Para endpoint Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

3.1.3.2.12. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

3.1.3.2.13. Em endpoint Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

3.1.3.2.14. A solução deverá mostrar a data do último scan realizado, tenha sido ele agendado ou manual;

3.1.3.2.15. Deve possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

3.1.3.2.16. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no sistema;

3.1.3.2.17. A solução deve ser capaz de tentar forçar a comunicação com o agente.

3.1.3.2.18. A solução deverá ter a capacidade de escanear drivers de rede mapeados nos servidores.

3.1.3.3. Funcionalidade de proteção contra URL's Maliciosas

3.1.3.3.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

3.1.3.3.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo o bloqueio de URLs com baixa reputação;

3.1.3.3.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas, e deve permitir também a criação de blacklists e whitelists de URL's;

3.1.3.3.4. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

3.1.3.3.5. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

3.1.3.3.6. A solução deve permitir que o administrador reclassifique uma URL para evitar falsos positivos.

3.1.3.4. Funcionalidade de Controle de Dispositivos

3.1.3.4.1. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por política e endpoint;

3.1.3.4.2. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, apenas leitura e bloqueio total;

3.1.3.4.3. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

3.1.3.4.4. Os eventos de bloqueio devem ser registrados em log.

3.1.3.5. Funcionalidade de Firewall

3.1.3.5.1. A solução deve ter a funcionalidade "Firewall de Host";

3.1.3.5.2. A solução deve ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

3.1.3.5.3. A solução deve ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

3.1.3.5.4. A solução deve ter a capacidade de definir regras distintas para interfaces de rede distintas;

3.1.3.5.5. A solução deverá ser capaz de identificar e possibilitar o bloqueio a endereços IP que estejam realizando escaneamento de rede, portas, protocolos e outras formas de reconhecimento;

3.1.3.5.6. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

3.1.3.5.7. A solução deverá possibilitar a criação de regras de bloqueio ou liberação, utilizando parâmetros como por exemplo: endereço IP, endereço MAC, portas de comunicação, protocolo, etc;

3.1.3.5.8. As regras de firewall poderão ou não ser válidas de acordo com agendamento por

horário ou dia da semana;

3.1.3.5.9. O firewall deverá ser stateful bidirecional;

3.1.3.5.10. O firewall deverá permitir liberar ou apenas logar eventos;

3.1.3.5.11. As regras de Firewall deverão ter ao menos as seguintes ações, ou equivalentes: Allow, deny e log only;

3.1.3.5.12. A solução deverá gerar logs das atividades stateful;

3.1.3.5.13. A solução deverá prevenir ack storm.

3.1.3.6. Funcionalidade de IPS para Estações de Trabalho

3.1.3.6.1. A solução deve possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

3.1.3.6.2. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

3.1.3.6.3. A solução deve ter a capacidade de detectar uma conexão maliciosa e bloqueá-la;

3.1.3.6.4. A solução deve ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

3.1.3.6.5. A solução deverá ser capaz de configurar as ações automáticas de proteção com base no perfil ou host;

3.1.3.6.6. As regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

3.1.3.6.7. A solução deverá ser capaz de inspecionar tráfego criptografado de entrada;

3.1.3.6.8. As regras de proteção contra vulnerabilidades deverão conter links com referências externas (quando aplicável), explicando a vulnerabilidade do fabricante ou CVE relacionado;

3.1.3.6.9. A solução deverá identificar e proteger de vulnerabilidades para as quais o fabricante ainda não tenha correção (patch);

3.1.3.6.10. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

3.1.3.6.11. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

3.1.3.6.12. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

3.1.3.6.13. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

3.1.3.6.14. As regras de IPS devem ser atualizadas automaticamente pelo fabricante.

3.1.3.7. Funcionalidade de controle de aplicações

3.1.3.7.1. As regras de controle de aplicação devem permitir as seguintes ações: liberar e bloquear;

3.1.3.7.2. A regra com permissão de liberar aplicações deve possuir as seguintes funcionalidades: permitir a execução de processos externos, não permitir a execução de processos externos e herdar direitos de execução;

3.1.3.7.3. O módulo de controle de aplicações deve permitir importar e exportar regras;

3.1.3.7.4. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

3.1.3.7.5. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: Assinatura sha-1 e sha-256 do executável;

3.1.3.7.6. Atributos do certificado utilizado para assinatura digital do executável, Caminho lógico do executável, Base de assinaturas de certificados digitais válidos e seguros;

3.1.3.7.7. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

3.1.3.7.8. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

3.1.3.7.9. O modulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionadas para bloqueio e monitoramento.

3.2. Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para servidores. Incluídos: instalação, configuração e suporte por 36 meses (item 2)

3.2.1. A solução deverá ser compatível com no mínimo os sistemas operacionais:

3.2.1.1. Windows:

3.2.1.1.1. Windows Server 2008 (32/64-bit);

3.2.1.1.2. Windows Server 2012 (64-bit);

3.2.1.1.3. Windows Server 2016 (64-bit);

3.2.1.1.4. Windows Server 2019 (64-bit);

3.2.1.1.5. Windows Server 2022 e posteriores.

3.2.1.2. Linux:

3.2.1.2.1. Red Hat Enterprise Linux 6, 7, 8 (64-bit) e posteriores;

3.2.1.2.2. CentOS 6, 7, 8 e posteriores;

3.2.1.2.3. Oracle Linux 5, 6, 7, 8 e posteriores

3.2.1.2.4. Red Hat Enterprise Linux 9 (64-bit) e posteriores;

3.2.1.2.5. SUSE Linux Enterprise Server 15 (64-bit) e posteriores;

3.2.1.2.6. Ubuntu 18, 20, 22 e posteriores;

3.2.1.2.7. Debian 8, 9, 10, 11 e posteriores.

3.2.2. A solução deverá permitir gerenciar políticas de segurança em múltiplas plataformas e sistemas operacionais, para hosts físicos e virtuais, todos em uma única console centralizada e do mesmo fabricante;

3.2.3. A solução deverá permitir no mínimo a aplicação de regras de IPS/IDS e antimalware para hosts gerenciados de Docker container;

3.2.4. A solução deverá possuir gerenciamento de todos os eventos relativos aos hosts gerenciados possibilitando, além do armazenamento dos eventos na própria solução, o seu encaminhamento para uma solução de SIEM;

3.2.5. Desejável que a solução tenha a capacidade de se integrar com os principais softwares de SIEMs de mercado, como por exemplo: Ossim, IBMQradar, Splunk e ArcSight, de modo a permitir enviar os seus logs para essas soluções;

3.2.6. Deverá possibilitar enviar logs para SYSLOG servers;

3.2.7. Deverá suportar o uso de RESTful API para permitir a integração com outras aplicações;

3.2.8. Deverá suportar o uso de RESTful API para permitir automatizações operacionais de tarefas;

3.2.9. O uso de RESTful API deve suportar no mínimo as seguintes automatizações:

3.2.9.1. Executar tarefas de manutenção de rotina;

3.2.9.2. Configurar políticas e proteger servidores;

3.2.9.3. Pesquisar políticas por nome.

3.2.10. Proteção Antimalware

3.2.10.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

3.2.10.2. A solução deve ter a capacidade de definir em quais diretórios do sistema serão realizadas varreduras para ameaças;

3.2.10.3. A solução deve possuir listas de exclusão separadas por funcionalidade da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

3.2.10.4. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

3.2.10.5. Em endpoints Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

3.2.10.6. A solução deverá ter a capacidade de monitorar o comportamento do sistema, de modo a detectar mudanças e atividades suspeitas não autorizadas;

3.2.10.7. A solução deverá ser capaz de escanear processos em memória, a fim de detectar Malwares;

3.2.10.8. Deverá ser possível configurar os níveis de camadas de compressão para a varredura de arquivos comprimidos;

3.2.10.9. Deverá realizar varredura de arquivos comprimidos do tipo OLE, sendo possível configurar as camadas de compressão;

3.2.10.10. A solução deve permitir iniciar ou cancelar escaneamento manual a partir de uma notificação recebida no endpoint;

3.2.10.11. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

3.2.10.12. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

3.2.10.13. Em endpoint Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

3.2.10.14. A solução deverá mostrar a data do último scan realizado, tenha sido ele agendado ou manual;

3.2.10.15. Deve possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

3.2.10.16. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no sistema;

3.2.10.17. A solução deve ser capaz de tentar forçar a comunicação com o agente.

3.2.10.18. A solução deverá ter a capacidade de escanear drivers de rede mapeados nos servidores.

3.2.11. Proteção contra URL's Maliciosas

3.2.11.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

3.2.11.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo o bloqueio de URLs com baixa reputação;

3.2.11.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas, e deve permitir também a criação de blacklists e whitelists de URL's;

3.2.11.4. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

3.2.11.5. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

3.2.11.6. A solução deve permitir que o administrador reclassifique uma URL para evitar falsos positivos.

3.2.12. Controle de Dispositivos

3.2.12.1. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por política e endpoint;

3.2.12.2. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, apenas leitura e bloqueio total;

3.2.12.3. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

3.2.12.4. Os eventos de bloqueio devem ser registrados em log.

3.2.13. Firewall

3.2.13.1. A solução deve operar também como firewall de host, através da instalação de agentes nos endpoints protegidos;

3.2.13.2. A solução deve ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

3.2.13.3. A solução deve ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

3.2.13.4. A solução deve ter a capacidade de definir regras distintas para interfaces de rede distintas;

3.2.13.5. A solução deverá ser capaz de identificar e possibilitar o bloqueio a endereços IP que estejam realizando escaneamento de rede, portas, protocolos e outras formas de reconhecimento;

3.2.13.6. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

3.2.13.7. A solução deverá possibilitar a criação de regras de bloqueio ou liberação, utilizando parâmetros como por exemplo: endereço IP, endereço MAC, portas de comunicação, protocolo, etc;

3.2.13.8. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

3.2.13.9. As regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

3.2.13.10. O firewall deverá ser stateful bidirecional;

3.2.13.11. O firewall deverá permitir liberar ou apenas logar eventos;

3.2.13.12. As regras de Firewall deverão ter ao menos as seguintes ações, ou equivalentes: Allow, deny e log only;

3.2.13.13. A solução deverá gerar logs das atividades stateful;

3.2.13.14. A solução deverá prevenir ack storm.

3.2.14. IPS

3.2.14.1. A solução deve possuir a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

3.2.14.2. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

3.2.14.3. A solução deve ter a capacidade de detectar uma conexão maliciosa e bloqueá-la;

3.2.14.4. A solução deve ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

3.2.14.5. A solução deverá ser capaz de configurar as ações automáticas de proteção com base no perfil ou host;

3.2.14.6. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

3.2.14.7. As regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

3.2.14.8. A solução deverá ser capaz de inspecionar tráfego criptografado de entrada;

3.2.14.9. As regras de proteção contra vulnerabilidades deverão conter links com referências externas (quando aplicável), explicando a vulnerabilidade do fabricante ou CVE relacionado;

3.2.14.10. A solução deverá identificar e proteger de vulnerabilidades para as quais o fabricante ainda não tenha correção (patch);

3.2.14.11. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

3.2.14.12. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

3.2.14.13. As regras de IPS poderão ter sua capacidade de LOG desabilitado;

3.2.14.14. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta;

3.2.14.15. As regras de IPS devem ser atualizadas automaticamente pelo fabricante.

3.2.15. Configurações de Controle de Aplicações

3.2.15.1. A solução deve ter a funcionalidade de controle de aplicações;

3.2.15.2. A solução deve ser capaz de bloquear softwares não reconhecidos;

3.2.15.3. A solução deve ser capaz de gerar relatório referente ao status do módulo;

3.2.14.4. A solução deve ser capaz de gerar relatório sobre o status do agente;

3.2.15.5. A solução deve ser capaz de gerar script de instalação do agente;

3.2.15.6. Monitoração de Status - Visualização do status dos hosts gerenciados, incluindo a realização de healthcheks.

3.2.15.7. A solução deverá permitir a entrega de agentes por pelo menos uma dentre as

principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet.

3.2.16. Monitoramento de Integridade e Rastreabilidade

3.2.16.1. Deverá possuir monitoramento de integridade e rastreabilidade baseada em agente;

3.2.16.2. O monitoramento de integridade e rastreabilidade deverá ser realizado em tempo real;

3.2.16.3. Deverá detectar mudanças de integridade em arquivos e diretórios do sistema operacional e aplicações terceiras;

3.2.16.4. Deverá detectar mudanças no estado de portas em sistemas operacionais Linux;

3.2.16.5. Deverá monitorar o status de serviços e processos do sistema operacional;

3.2.16.6. Deverá monitorar mudanças efetuadas no registro do Windows;

3.2.16.7. Deverá possibilitar customização de regras para monitoramento de integridade e rastreabilidade em chaves de registro, diretórios e subdiretórios;

3.2.16.8. Deverá possibilitar customização de XML para criação de regras monitoramento de integridade avançadas;

3.2.16.9. Deverá realizar auditoria no sistema operacional e aplicações (agendada e manual), para destacar e atribuir automaticamente a regra relevante para monitoramento de integridade de acordo com o resultado dessa auditoria;

3.2.16.10. Deverá habilitar e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (caso a área monitorada não seja mais importante, a regra deverá ser removida automaticamente; e vice-versa);

3.2.16.11. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

3.2.16.12. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

3.2.16.13. A solução deverá monitorar modificações em arquivos, pastas, registros, processos, serviços e portas;

3.2.16.14. Deverá possibilitar o rastreamento de arquivos por criação, última modificação, último acesso, permissões, owner, grupo, tamanho, SHA1, SHA256 e Flags;

3.2.16.15. Deverá possibilitar gerar alertas toda vez que uma modificação ocorrer, em tempo real para ambiente Windows e, pseudo tempo real para ambiente Linux utilizando agente;

3.2.16.16. Deverá ser possível gerar relatório de todas as modificações que ocorram nos objetos monitorados;

3.2.16.17. Deverá classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

3.2.16.18. Deverá possibilitar definir o diretório onde o arquivo será monitorado, possibilitando inclusão ou não de determinados tipos de arquivos dentro desse mesmo diretório;

3.2.16.19. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

3.2.16.20. Deverá possibilitar classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas.

3.2.17. Inspeção de Logs

3.2.17.1. Deverá monitorar e inspecionar arquivos de log do sistema operacional e demais

aplicações, armazenando uma cópia desses logs em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

3.2.17.2. Deverá realizar auditoria no sistema operacional e aplicações (agendada e manual), para destacar e atribuir automaticamente a regra relevante para inspeção de logs de acordo com o resultado dessa auditoria;

3.2.17.3. Deverá habilitar e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (caso a área monitorada não seja mais importante, a regra deverá ser removida automaticamente; e vice-versa);

3.2.17.4. Deverá permitir customização de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;

3.2.17.5. Deverá permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;

3.2.17.6. Deverá possuir inteligência de alertas para cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente e/ou do servidor;

3.2.17.7. Deverá permitir modificar as regras por severidade de ocorrência de eventos;

3.2.17.8. Deverá suportar sintaxe OSSEC padrão aberto;

3.2.17.9. Deverá suportar tipos comuns de log de eventos (log de eventos, snort, syslog e outros ...)

3.2.17.10. Deverá possuir decodificadores predefinidos para tipos comuns de log de eventos com base no regex.

3.2.18. Controle de Aplicações

3.2.18.1. Deverá realizar inventário de softwares instalados e criar um conjunto de regras local e/ou um conjunto de regras compartilhado via API;

3.2.18.2. Deverá possuir as seguintes configurações ou semelhante:

3.2.18.2.1. Bloqueio: possibilitando o bloqueio de aplicações, impedindo a execução de todos os softwares novos ou alterados, a menos que sejam expressamente permitidos;

3.2.18.2.2. Permitido: possibilitando que aplicações sejam executadas por padrão, a menos que sejam expressamente bloqueadas;

3.2.18.3. Deverá possuir lista de permissões de inventário, ou seja, ao ativar o controle de aplicações, todos os softwares atualmente instalados devem ser adicionados à lista de permissões do inventário do servidor e pode ser executado;

3.2.18.4. Deve ser possível configurar modo de manutenção possibilitando instalar ou atualizar a lista de softwares permitidos na lista de inventário;

3.2.18.5. Deverá monitorar continuamente o servidor quanto as alterações. Devendo ser integrado ao kernel e ao sistema de arquivos, monitorando todo o servidor, incluindo o software instalado pelas contas root e de administrador.

3.2.18.6. Deverá detectar novos softwares, comparando hash, tamanho do arquivo, nome do arquivo e pasta;

3.2.18.7. Deve também realizar o controle de aplicativos em:

3.2.18.7.1. Aplicações Windows (.exe, .com, .dll, .sys), bibliotecas Linux (.so) e outros binários e bibliotecas compilados

3.2.18.7.2. Arquivos Java .jar e .class e outro código de bytes compilado

3.2.18.7.3. Scripts PHP, Python e shell, além de outros aplicativos e scripts da web que são interpretados ou compilados em tempo real

3.2.18.7.4. Scripts do Windows PowerShell, batch (.bat) e outros scripts específicos do

Windows (.wsf, .vbs, .js)

3.2.18.8. Deverá exibir todos os softwares não reconhecidos, ou seja, softwares que não estão na lista de permissões de inventário de um servidor e não possuem uma regra de controle de aplicação correspondente, possibilitando tomar a ação de "Permitir" ou "Bloquear".

3.2.19. Gerenciamento

3.2.19.1. A solução deverá ser gerenciada por console Web, devendo suportar certificado digital para gerenciamento;

3.2.19.2. O gerenciamento da console web deverá suportar no mínimo, as versões atuais dos seguintes navegadores: Firefox, Microsoft Edge, Google Chrome e Safari;

3.2.19.3. A solução EDR do item 2 deverá ser gerenciada através de painel centralizado, disponibilizado na nuvem da Contratada ou do Fabricante da Solução, onde o acesso ocorrerá de maneira criptografada (SSL/TLS). Alternativamente, este painel poderá ser posicionado dentro da infraestrutura da Contratante, que será então responsável pelos equipamentos físicos ou virtuais onde o componente será instalado. No caso de gerenciamento on premise, a console/ painel deverá ser compatível com a instalação no Windows Server 2016 e posteriores, e com o RHEL 7, 8 e posteriores;

3.2.19.4. Na alternativa on premise, a solução deve suportar base de dados Microsoft SQL Server;

3.2.19.5. A console de gerenciamento deverá disponibilizar os pacotes de instalação de agentes para todos os sistemas operacionais suportados, provendo inclusive scripts de instalação de agents (power shell script e bash script);

3.2.19.6. Deverá permitir o envio de registros de logs a um servidor remoto;

3.2.19.7. Deverá suportar o envio ao menos nos seguintes formatos: Raw Syslog, CEF e LEEF;

3.2.19.8. Deverá suportar integração com serviços de terceiros baseando-se em SAML 2.0 para serviços como ADFS, Okta, PingOne entre outros;

3.2.19.9. Desejável suportar APIs abertas para integração com serviços de terceiros;

3.2.19.10. A comunicação entre a console de gerenciamento e componentes de proteção deverá ser criptografada;

3.2.19.11. Deverá armazenar os eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;

3.2.19.12. Deverá permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;

3.2.19.13. A console deverá ter a capacidade de se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução, com permissões customizadas pela própria solução;

3.2.19.14. Deverá armazenar políticas e logs em base de dados, suportando, no mínimo, bancos de dados:

3.2.19.14.1. PostgreSQL

3.2.19.14.2. Microsoft SQL Server

3.2.19.14.3. Oracle database.

3.2.19.15. Deverá permitir a definição de permissionamento, no mínimo, para os modos de visualização e edição de políticas;

3.2.19.16. Deverá permitir a atribuição granular de permissões para servidores gerenciados, podendo delimitar quais os servidores que podem ser visualizados e gerenciados para cada usuário ou grupo de usuários;

3.2.19.17. Deverá possuir dashboards para facilidade de monitoração, as quais poderão ser customizados pelo usuário em quantidade de dashboards e período de monitoração;

3.2.19.18. Deverá ser possível criar políticas de forma global para todas os servidores, por perfis e individualmente para cada host;

3.2.19.19. Deverá permitir a criação/utilização de tags pré-definidas para o agrupamento e aplicação de políticas aos hosts segundo características comuns;

3.2.19.20. Deverá permitir o envio de eventos da console via SNMP;

3.2.19.21. Permitir o rollback de atualização de regras pela console de gerenciamento;

3.2.19.22. Deverá gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

3.2.19.23. Deverá possuir a capacidade de marcar eventos (tags) de modo a facilitar o gerenciamento, relatórios e visualização;

3.2.19.24. Deverá classificar eventos para facilitar a identificação e a visualização de eventos críticos em servidores críticos.

3.2.19.25. Deverá permitir o gerenciamento agrupando os hosts em pastas inteligentes, possibilitando organização de grupos de hosts para a aplicação de políticas. O agrupamento de hosts deverá ser no mínimo pelos seguintes parâmetros:

3.2.19.25.1. Hostname;

3.2.19.25.2. Sistema Operacional;

3.2.19.25.3. Docker Host;

3.2.19.25.4. Política de Configurações;

3.2.19.25.5. Active Directory Name/Folder.

3.2.19.26. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

3.2.19.27. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

3.2.19.28. A solução deve ser capaz de realizar a administração de contas – executando a criação, edição e exclusão de contas de acesso.

3.2.19.29. Quando implementado em modo alta disponibilidade, as consoles devem compartilhar o mesmo banco de dados.

3.3. Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para dispositivos móveis. Incluídos: instalação, configuração e suporte por 36 meses (item 3)

3.3.1. O módulo de proteção de dispositivos móveis deve possuir agente para os seguintes sistemas operacionais:

3.3.1.1. Android 9.0 em diante;

3.3.1.2. iOS 11 em diante.

3.3.2. As funcionalidades deverão estar disponíveis de acordo com cada plataforma;

3.3.3. Deve possuir proteção de antimalware utilizando assinaturas e machine learning;

3.3.4. Deve ser capaz de realizar escaneamento de malwares em tempo real, do cartão sd e após atualização de vacinas;

3.3.5. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de números bloqueados para recebimento de chamadas;

3.3.6. Deve possuir funcionalidade de filtro de chamadas que possibilita a criação de lista de números permitidos para efetuação de chamadas;

3.3.7. Deve possuir a funcionalidade de firewall para bloqueio de tráfego de entrada e saída;

3.3.8. Deve permitir a proteção contra ameaças provenientes da web por meio de um sistema de reputação de segurança das URL's acessadas;

3.3.9. Deve permitir o controle de acesso a websites por meio de listas de bloqueio e aprovação;

3.3.10. Controle da política de segurança de senhas, com critérios mínimos de: Padrão de senha; Uso obrigatório de senha; tamanho mínimo; Tempo de expiração; Bloqueio automático da tela; Bloqueio por tentativas inválidas;

3.3.11. Controle de acesso à seguinte lista funções e status de ativação de funções dos dispositivos móveis: Bluetooth, Câmera, Cartões de memória, Wlan/wifi, GPS, Alto-falante, Armazenamento USB, Rede Móvel, Modo de desenvolvedor, Ancoragem (tethering);

3.3.12. Deve possuir engine para detecção e bloqueio de ransomware;

3.3.13. Deve realizar scan de vulnerabilidades no smartphone;

3.3.14. Deve monitorar a conexão wi-fi e notificar o usuário caso a conexão não seja segura;

3.3.15. Deve permitir o bloqueio de aplicativos;

3.3.16. Deve verificar se o smartphone está em modo root (Android);

3.3.17. Deve verificar se o smartphone está com jailbreak (iOS);

3.3.18. A proteção para smartphones e tablets deverá identificar aplicativos maliciosos oferecendo sugestões de ações;

3.3.19. Deve possuir integração com o gerenciamento unificado para visibilidade dos dispositivos moveis, single sign on e recebimento de políticas.

3.4. Subscrição de licenças de uso para solução de proteção a aplicações em nuvem. Incluídos: instalação, configuração e suporte por 36 meses (item 4)

3.4.1. A solução deve permitir a identificação e proteção contra ameaças, ao menos nas seguintes soluções em nuvem:

3.4.1.1. Microsoft 365 no mínimo Exchange Online, Sharepoint Online, Onedrive for Business e Microsoft Teams;

3.4.1.2. Gsuite.

3.4.2. Deve bloquear caso o usuário tente fazer o upload de um determinado arquivo malicioso ou proibido nas plataformas: Onedrive, Sharepoint, Microsoft Teams e Gsuite;

3.4.3. Bloquear upload de arquivos por tipo definido em política para as soluções supracitadas;

3.4.4. Identificar e bloquear URLs maliciosas em arquivos e URLs, incluindo URLs inseridas em anexos;

3.4.5. Deve ser possível realizar escaneamento do Exchange ou Gmail de forma manual para identificação de possíveis ameaças e arquivos maliciosos;

3.4.6. Deve ser possível configurar os destinatários para o recebimento dos resultados do escaneamento;

3.4.7. Deve permitir realizar escaneamento retroativo de ameaças sob demanda, isto é, em busca de ameaças já armazenadas;

3.4.8. Deve ser possível configurar o nível de sensibilidade das URLs maliciosas;

3.4.9. Deve ser possível cadastrar os usuários importantes com objetivo de analisar e identificar possíveis e-mails de fraude baseado em comportamento e padrão de escrita;

3.4.10. Deve permitir que os administradores configurem a periodicidade das notificações para, no mínimo, URLs maliciosas identificadas, SPAMs maliciosos, Phishing, Ransomware, arquivos analisados na sandbox e identificados como alto e médio risco;

3.4.11. A solução deve permitir a visualização das estatísticas no dashboard por serviço integrado (Exchange Online, Teams, Onedrive, Sharepoint e Gsuite);

3.4.12. Deve ser possível ajustar o período dos logs para análise;

3.4.13. Deve ter a capacidade de analisar arquivos e URLs em sandbox para identificação de ameaças desconhecidas (sem assinatura);

3.4.14. Deve utilizar mecanismos de proteção que contemplem, pelo menos, malwares conhecidos por assinatura, malwares desconhecidos por Machine Learning, bloqueio de conteúdo (por tipo de arquivo, por exemplo), reputação de URLs;

3.4.15. A solução deve permitir compartilhamento de informações através de SIEM via API ou através da gerência centralizada;

3.4.16. A solução deve prover relatórios que contemplem, pelo menos, riscos de segurança, ameaças, ransomware, arquivos analisados em sandbox, auditoria e API;

3.4.17. Os relatórios devem ser exportáveis para, pelo menos, PDF;

3.4.18. A verificação Anti-malware deverá permitir a customização das ações a serem tomadas, por exemplo: quarentenar, deletar e passar.

3.4.19. Aplicar proteções anti-malware, verificação de URL’s maliciosas para a proteção dos serviços.

3.4.20. Aplicar proteções contra Comprometimento de E-mail utilizando análise de escrita;

3.4.21. Deve permitir a integração nuvem-a-nuvem, através de API com, no mínimo, as seguintes aplicações: Microsoft 365, Dropbox e Google, realizando a análise de malware em sandbox;

3.4.22. Deve ser possível configurar o envio de notificação por e-mail para administradores, caso haja execução da regra e bloqueio ou quarentena como ação de resposta;

3.4.23. Os alertas enviados deverão permitir a customização tanto para o usuário quanto para o administrador;

3.4.24. Monitorar em tempo real para bloquear arquivos e, caso configurado, colocá-los em quarentena;

3.4.25. Empregar detecção de malware por meio de sandbox sem assinaturas, para diminuir seu risco de violação;

3.4.26. Monitorar o comportamento real de arquivos suspeitos em ambientes sandbox virtuais, usando múltiplas versões de sistemas operacionais e aplicações;

3.4.27. As políticas deverão possuir a capacidade de serem realizadas por usuário ou grupo;

3.4.28. Possuir um dashboard com as principais ameaças detectadas, a exemplo dos tipos Ransomware, Phishing, Comprometimento de E-mail;

3.4.29. A solução deverá ser capaz de implementar políticas para prevenção contra envio de informações sensíveis armazenados nas aplicações em nuvem;

3.4.30. A Sandbox deverá ter a opção para funcionar em modo de monitoramento, não tomando nenhuma ação nos arquivos detectados;

3.4.31. Deverá possui a funcionalidade de verificação de SPAM com níveis de detecções diferentes;

3.4.32. As ações realizadas pelo antispam deverão possuir ao menos as seguintes opções: quarentenar, adicionar uma tag no assunto, deletar ou mover para a pasta de lixo;

3.4.33. Deverá permitir o administrador adicionar ou bloquear um endereço na lista de remetentes.

3.5. Subscrição de licenças de uso para solução de Proteção a servidores de e-mail. Incluídos: instalação, configuração e suporte por 36 meses (item 5)

3.5.1. Deve fornece proteção abrangente para phishing, spam e graymail com várias técnicas, incluindo análise de remetente, conteúdo e imagem, Deve associar técnicas de aprendizado de máquina na análise das vulnerabilidades citadas;

3.5.2. Deve realizar analisar de cabeçalho e conteúdo;

3.5.3. Deve realizar análise em documentos para detectar malware e vulnerabilidade em arquivos do tipo PDFs, txt, documentos office (Microsoft e Libreoffice). Nesta análise deve usar técnicas de estática e heurística para detectar e examinar anormalidades;

3.5.4. Deve utilizar tecnologia sandbox para análise dinâmica de anexos potencialmente maliciosos ou URLs enviadas junto ao e-mail;

3.5.5. Deve analisar e extrair arquivos protegidos por senha de forma heurística. Para isso deve combinar senhas definidas pelo usuário e conteúdo da mensagem;

3.5.6. Deve bloqueia e-mails com URLs mal-intencionados antes da entrega e verificar novamente a segurança da URL quando um usuário clicar na mesma;

3.5.7. Deve analisar a autenticação do remetente por: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting, and Conformance);

3.5.8. Deve possuir banco de dados de ameaças para correlacionar vulnerabilidades;

3.5.9. Deve possuir tecnologia de criptografia de e-mails orientada por políticas, incluir o serviço de gerenciamento de chaves privadas e permite que os destinatários leiam e-mails criptografados em qualquer dispositivo usando um navegador Web;

3.5.10. Deve incluir técnicas para facilitar o rastreamento, a documentação e a proteção de informações confidenciais;

3.5.11. Em caso de interrupção do servidor de e-mail, a solução deve garantir a continuidade do serviço de e-mail, garantindo o recebimento dos e-mails e os colocando em espera até o restabelecimento do servidor de e-mail;

3.5.12. Deve possuir gerencia centralizada na qual seja possível exportar relatórios sobre o serviço;

3.5.13. Deve possuir entrega de relatórios personalizados e programados;

3.5.14. Deve possuir integração para exportação de logs para ferramentas do tipo Syslog.

3.5.15. Sobre a solução anti-phishing e spam:

3.5.15.1. Deve examinar a autenticidade e a reputação do remetente de e-mail para filtrar remetentes mal-intencionados;

3.5.15.2. Deve analisar o conteúdo do e-mail em busca de vulnerabilidades;

3.5.15.3. Deve proteger contra URLs mal-intencionados na entrega do e-mail ao usuário e no momento que o usuário clicar na mesma, bloqueando em caso de possuir links de URLs mal-intencionadas;

3.5.16. Sobre ameaças avançadas:

3.5.16.1. Deve detectar e bloquear ransomware e outros tipos de malware de dia zero, para isso deve utilizar técnicas de aprendizado de máquina de pré-execução, análise de macros, detecção de

exploração e análise dinâmica de sandbox para arquivos e URLs;

3.5.16.2. A ferramenta deve possuir integração com os outros componentes da solução de segurança presente no lote único, de modo a compartilhar informações sobre ameaças, assim garantindo maior segurança contra ataques persistentes e direcionados;

3.5.16.3. Deve permitir a criação de lista de usuários da organização para implementar a proteção de e-mail a estas contas caso não se opte por adotar a proteção em todas as contas de e-mail.

3.6. Subscrição de licenças de uso para solução de visibilidade, detecção, investigação e alertas de incidentes (XDR). Incluídos: instalação, configuração e suporte por 36 meses. (item 6)

3.6.1. A solução deve ser capaz de agregar em sua plataforma de segurança os itens 1, 2, 3, 4 e 5 do objeto, permitindo o gerenciamento e monitoramento unificado de toda a solução tecnológica contratada;

3.6.2. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise de impacto e análise de causa-raiz;

3.6.3. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

3.6.4. Deve exibir todos os detalhes do incidente em uma única página, contendo no mínimo: status do incidente, escopo do impacto: quantidade de estações de trabalho impactadas, quantidade de servidores impactados, quantidade de usuários impactados, quantidade de contas de e-mails impactadas, data e hora, modelo de detecção e objetos detectados;

3.6.5. Deve permitir alterar os status de cada evento;

3.6.6. Permitir adicionar comentários e notas a cada evento pelos analistas da ferramenta;

3.6.7. A investigação deve permitir a análise do recebimento, execução de arquivos, processos, sessões de rede além de registro do Windows;

3.6.8. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

3.6.9. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

3.6.10. Detecção de Ameaça

3.6.10.1. A solução deve apresentar uma lista com todos os modelos de detecção pré-definidos que a solução possui;

3.6.10.2. Cada modelo deve possuir uma descrição para auxiliar na identificação do risco e impacto de cada modelo;

3.6.10.3. Deve permitir ativar ou desativar qualquer modelo de detecção caso necessário;

3.6.10.4. Permitir criação de listas de exceção de objetos para redução de falso-positivo.

3.6.10.5. Os modelos de detecção deverão possuir níveis de severidade individuais para cada modelo;

3.6.11. Threat Intelligence

3.6.11.1. Deve prover relatórios de inteligência de ameaças avançadas mais recentes e indicadores de comprometimento para ajudar sua organização a se defender proativamente contra ameaças;

3.6.11.2. Deve ser possível identificar individualmente cada relatório de ameaça;

3.6.11.3. Deve permitir adicionar bases de inteligência terceiras de forma manual, por API, importando arquivos com base CSV ou STIX através de assinatura de feeds de inteligência de ameaças terceiros;

3.6.11.4. Deve permitir adicionar no mínimo os seguintes indicativos de comprometimento (IOCs) à base de inteligência: Arquivos SHA-1, URLs, IPs e Domínios;

3.6.11.5. Deve permitir configurar as ações dos indicativos de comprometimento (IOCs) adicionados à console em pelo menos: Bloquear, Quarentenar e Log;

3.6.12. Investigação de Incidentes

3.6.12.1. Capacidade de construir sequências de buscas para localizar os dados ou objetos em seu ambiente que você deseja examinar;

3.6.12.2. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta para identificar e categorizar os resultados da pesquisa;

3.6.12.3. O campo de busca deve permitir o uso de múltiplos operadores lógicos, além de permitir indexar múltiplas buscas;

3.6.12.4. Deve permitir salvar pesquisas com os critérios de busca e operadores lógicos utilizados para futuras consultas;

3.6.12.5. Deve permitir realizar buscas de objetos para pelo menos os seguintes critérios: nome de domínio, remetente do e-mail, IPv6, endpoint ID, Conta de usuário, Nome do arquivo, porta, URL, arquivo SHA-1, arquivo SHA-2, caminho do arquivo e arquivo MD5;

3.6.12.6. Deve enviar alertas de notificação por email;

3.6.12.7. Deve correlacionar atividades para identificação de ataques;

3.6.12.8. Deve possuir recursos de “machine learning” para identificação de ameaças;

3.6.12.9. Deve ser possível desabilitar regras específicas conforme necessidade;

3.6.12.10. Deve possuir recurso para visualizar os resultados de investigação das detecções, possibilitando verificar o status;

3.6.12.11. Deve possuir visualização do ataque com gráficos para análise avançada com no mínimo os seguintes recursos:

3.6.13. Visualização das ações da ameaça

3.6.13.1. Análise de rede para repetição das comunicações e visualização das comunicações e tráfego lateral.

3.6.13.2. Deve possuir mecanismo de descoberta para os seguintes vetores:

3.6.13.2.1. Endpoint;

3.6.13.2.2. Rede.

3.6.13.3. Deve possuir mecanismo de busca de ameaças customizados e IoC (indicadores de comprometimento);

3.6.13.4. Após a busca, deve ser possível iniciar uma investigação através da console de gerência;

3.6.13.5. O Fabricante deve possuir base de inteligência integrada com a solução para detecção automática de ameaças com indicadores de IoC (Indicadores de Comprometimento);

3.6.13.6. Deve fornecer informações das ameaças conforme o framework do MITRE ATT&CK, e prover links com informações associadas ao referido framework sobre as ameaças encontradas;

3.6.13.7. Deve possuir mecanismo de alerta para incidentes através da solução de Gerência;

3.6.13.8. Deve possuir API's para integrações com soluções de SIEM e SOAR;

3.6.13.9. A solução deve ser compatível com os sistemas operacionais Windows (versão 8.1 e superiores), Linux (Debian 6 e superiores, Fedora 12 e superiores) e MacOS (Mac OS X 10.13 e

superiores);

3.6.13.10. A solução deve avaliar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

3.6.13.11. A solução deve possuir módulo de investigação e detecção integrados;

3.6.13.12. A solução deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;

3.6.13.13. A solução deve possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;

3.6.13.14. A solução deve utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

3.6.13.15. A solução deve apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;

3.6.13.16. A solução deve fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;

3.6.13.17. A solução deve ter a capacidade de construir sequências de buscas para localizar os dados ou objetos nos ambientes a serem examinados;

3.6.13.18. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;

3.6.13.19. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;

3.6.13.20. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise de impacto e análise de causa-raiz;

3.6.13.21. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

3.6.13.22. Deve permitir que as detecções sejam correlacionadas com todos os módulos da solução através de uma console dedicada. Esta console deverá ser preferencialmente do mesmo fabricante dos demais módulos da solução;

3.6.13.23. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;

3.6.13.24. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

3.6.13.25. O módulo de EDR deve atuar com base em modelos de detecção de ataques avançados e furtivos;

3.6.13.26. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

3.6.13.27. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;

3.6.13.28. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;

3.6.13.29. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise de impacto e análise de causa-raiz;

3.6.13.30. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;

3.6.13.31. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;

3.6.13.32. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

3.6.13.33. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

3.6.13.34. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;

3.6.13.35. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

3.6.13.36. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;

3.6.13.37. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;

3.6.13.38. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;

3.6.13.39. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;

3.6.13.40. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);

3.6.13.41. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;

3.6.13.42. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;

3.6.13.43. Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;

3.6.13.44. Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

3.6.13.45. Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

3.6.13.46. Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

3.6.13.47. Restaurar a conectividade da estação de trabalho com a rede;

3.6.13.48. Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;

3.6.13.49. Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

3.6.14. Mapeamento de Ativos

3.6.14.1. A solução XDR deverá ser capaz de realizar o mapeamento do inventário de ativos listados abaixo para construção da topologia do ambiente de cada Contratante:

3.6.14.2. Identificação de ativos internos e publicados na internet;

3.6.14.3. Identificação de serviços/tecnologias e suas versões;

3.6.14.4. Associação de serviços/tecnologias/servidores e seus endereços IPs;

3.6.14.5. As informações supracitadas são dinâmicas e serão atualizadas de forma constante, acompanhando alterações do ambiente e suas evoluções;

3.6.14.6. A Contratante fornecerá lista de ativos e sua classificação segundo criticidade e valor para o negócio. As informações devem ser utilizadas para priorizar as atividades de monitoramento,

alertas, prioridade de notificação, acompanhamento e ações, não estando restritas a somente essas e podendo ser alteradas a qualquer momento.

3.7. Serviço gerenciado de detecção e resposta (MDR) pelo período de 36 meses (item 7)

3.7.1. Características gerais do serviço MDR

3.7.1.1. O escopo do serviço gerenciado de detecção e resposta (MDR) deve abranger o monitoramento, detecção de incidentes de cibersegurança, análise, gerenciamento e envio de alertas e relatórios provenientes da solução XDR do Item 6, ficando então o serviço do Item 7, condicionado à contratação do referido Item 6;

3.7.1.2. A Contratada deverá manter em seu quadro de profissionais equipes que investiguem e analisem o comportamento de malware para desenvolver medidas de mitigação e aprimorar as defesas contra ameaças, além de disponibilizar profissionais qualificados na solução contratada para monitorar, coletar, analisar e reportar incidentes de segurança identificados, bem como suas formas de mitigação, nos ativos cobertos pelas licenças dos itens 1 a 6 do objeto. Todos os serviços prestados de gerenciamento de detecção e resposta deverão ser conduzidos por profissionais especializados na tecnologia contratada, atuando em nível 3. Entende-se por nível 3, especialistas altamente qualificados que possuem um conhecimento aprofundado sobre os produtos, sistemas e tecnologias suportadas no objeto do presente processo licitatório;

3.7.1.3. O serviço gerenciado de detecção e resposta à incidentes deve prover monitoramento contínuo dos ativos tecnológicos, com análises em tempo real e elaboração de relatórios de impacto, contendo os resultados das análises forenses, avaliando a extensão do ataque ou exploração de vulnerabilidades;

3.7.2. Características técnicas do serviço MDR

3.7.2.1. Monitoramento contínuo

3.7.2.1.1. O escopo dos ativos a serem monitorados no serviço MDR deverá ser definido durante a fase de instalação e configuração dos itens de subscrição, descrita no tópico 15.1 do ETP;

3.7.2.1.2. Ainda durante a fase de instalação e configuração citada no tópico anterior, a Contratante fornecerá lista de ativos e sua classificação segundo criticidade e valor para o negócio. As informações devem ser utilizadas para priorizar as atividades de monitoramento, alertas, prioridade de notificação, acompanhamento e ações, não estando restritas a somente essas e podendo ser alteradas a qualquer momento;

3.7.2.1.3. A Contratada deverá notificar a Contratante sobre quaisquer interrupções planejadas ou não planejadas relacionadas a: portal de serviços, os recursos de monitoramento ou funcionalidades relacionadas à capacidade da contratada de monitorar eventos;

3.7.2.1.4. A Contratada deverá promover pontos de verificação mensais de briefing (até uma (1) hora via teleconferência) para revisar relatórios, quaisquer alterações nos procedimentos de relatório, telemetria, processos, fluxos de trabalho e tecnologias.

3.7.2.2. Detecção, análise e mitigação de incidentes

3.7.2.2.1. A Contratada deverá identificar incidentes de Segurança da Informação que possam afetar a disponibilidade, integridade ou confidencialidade das informações existentes naqueles sistemas ou serviços de TIC da Contratante que estejam protegidos pelos componentes da solução ofertada.

3.7.2.2.2. A Contratada deverá utilizar as bases de inteligência de ameaças e a análise segura de malware para ajudar a identificar as ameaças mais recentes e relevantes, indicadores de ataque ou comprometimento e práticas recomendadas de mitigação, usando padrões/frameworks abertos como MITRE Att&ck, NIST NVD, etc;

3.7.2.2.3. A Contratada deverá estabelecer e demonstrar a adoção dos frameworks a serem utilizados em todas as etapas de identificação e tratativas de um ataque, com os respectivos controles para monitorar os avanços de um possível atacante em suas fases de Reconhecimento, Recursos de Infraestrutura, Acesso inicial, Execução, Persistência (ATP), Escalonamento de privilégios, Evasão, Acesso a credenciais, Descobrimento, Movimentação Lateral, Rastros e informações do invasor, Comando e Controle, Exfiltração e Impacto;

3.7.2.2.4. A Contratada deverá realizar periodicamente simulações e técnicas que evidenciem o perfeito funcionamento e atendimento aos requisitos de controle e detecção e resposta. A Contratada deverá gerar amostragem e evidencias das técnicas e atividades realizadas de tentativa de comprometimentos através de email, endpoint, diretórios e workloads, bem como o resultado da efetividade dos controles e o perfeito funcionamento da solução ofertada e seus playbooks de remediação;

3.7.2.2.5. A Contratada deverá acompanhar os alertas de segurança em tratamento à medida que evoluem ao longo do tempo, adicionando contexto ou detecções adicionais, conforme necessário e sempre que possível;

3.7.2.2.6. A Contratada deverá envolver-se com a Contratante em caso de incidente de segurança de alto risco (alerta positivo verdadeiro verificado). A Contratante fornecerá contexto sobre a gravidade da(s) ameaça(s), devendo a CONTRATADA fornecer insumos e recomendações à Contratante para que o mesmo conclua a correção final e a resolução do Incidente de Segurança;

3.7.2.2.7. A Contratada deverá responder a consultas da Contratante relacionadas a eventos/alertas de segurança ativos e informações contextuais relacionadas, como inteligência de ameaças ou impacto geral no ambiente ou nas operações da Contratante;

3.7.2.2.8. A Contratada deverá fornecer orientações sobre como mitigar, interromper ou prevenir um Incidente de segurança com base na inteligência e nos avisos fornecidos pela solução contratada, conforme relevância para o ambiente da Contratante. A resposta recomendada a um evento/incidente de segurança pode ser uma ou mais das seguintes:

3.7.2.2.8.1. Com a permissão da Contratante, realizar alterações de política ou configuração aprovadas nos componentes de segurança cobertos para ajudar a mitigar ou responder a incidentes de segurança;

3.7.2.2.8.2. Quando o incidente de segurança for um ataque conhecido, recomendar ações de resposta para ajudar a mitigar o ataque e fornecer orientação sobre como ajudar a remediar ainda mais o Incidente de segurança, aproveitando os componentes de segurança cobertos;

3.7.2.2.8.3. Onde for necessária uma validação adicional da ameaça, a Contratada fornecerá recomendações sobre áreas de foco para investigação do cliente;

3.7.2.2.8.4. Onde as ações de resposta estiverem fora dos componentes de segurança cobertos, a Contratada fornecerá ao cliente recomendações para investigação e correção adicionais;

3.7.2.2.9. A Contratada poderá, sempre que necessário, solicitar maior riqueza de informações que possam contribuir para uma investigação de segurança, tais como saídas de comandos, logs adicionais, acesso ao ativo, etc. A Contratante fornecerá tais informações caso seja viável ou pertinente;

3.7.2.2.10. Sempre que houver viabilidade técnica e operacional para a automação, desde que o escopo seja definido previamente levando em consideração possíveis impactos e desdobramentos da ação tomada, a Contratada poderá sugerir ações que reduzam o esforço operacional e implementem medidas preventivas, como por exemplo:

3.7.2.2.10.1. Isolamento de endpoint (isolar um computador do resto da rede, deixando apenas as conexões necessárias para acesso ao seu sensor pelo servidor de gerenciamento);

3.7.2.2.10.2. Bloquear automaticamente endereços IPs incluídos em listas de reputação públicas, ou de fontes de inteligência de ameaças ou oriundos de IOCs ou IOAs próprios da contratada, extraídos a partir de eventos e incidentes de segurança de outros clientes, desde que aferidos e definidos como maliciosos.

3.7.2.2.11. Investigar ameaças bloqueadas de alta prioridade para determinar quaisquer

informações e recomendações contextuais adicionais conforme necessário;

3.7.2.2.12. Investigar quaisquer ameaças não bloqueadas de média e alta prioridade e fornecer recomendações à Contratante em termos de alterações de política sugeridas ou ações de resposta;

3.7.2.2.13. Revisar periodicamente as ameaças não bloqueadas de baixa prioridade e fazer recomendações conforme necessário;

3.7.2.2.14. A Contratada deverá fazer recomendações a Contratante quanto a quaisquer ações de resposta a serem executadas nos terminais em resposta a uma ameaça identificada.

3.7.2.2.15. As informações citadas no subtópico 3.7.2.2.11. são dinâmicas e serão atualizadas de forma constante, acompanhando alterações do ambiente e suas evoluções;

3.7.2.2.16. A Contratante fornecerá lista de ativos e sua classificação segundo criticidade e valor para o negócio;

3.7.2.2.17. Realizar o monitoramento, a detecção e a notificação dos eventos apresentados pela solução contratada.

3.7.2.3. Relatórios e notificações

3.7.2.3.1. A Contratada deverá enviar à Contratante um relatório mensal contendo um resumo das ameaças de todos os níveis de severidade que foram identificadas naquele período, contendo ainda recomendações para mitigação, conforme necessário;

3.7.2.3.2. O relatório mencionado no tópico anterior servirá também para a finalidade de atestação do serviço prestado naquele período;

3.7.2.3.3. Diante da identificação de um incidente ou vulnerabilidade considerado crítico, a Contratada deverá emitir um relatório emergencial daquele incidente, contendo as evidências e orientações para a mitigação do problema;

3.7.2.3.4. Na ocasião das reuniões mensais do subtópico 3.7.2.1.4, o conteúdo dos relatórios mensais e emergenciais poderá ser redefinido pela Contratante, desde que seja viável;

3.7.2.3.5. O envio de relatórios de segurança contendo dados sigilosos sobre o ambiente da Contratante deve ser realizado utilizando meio criptografado;

3.7.2.3.6. A Contratada deverá notificar o contato da Contratante sobre eventos de segurança usando um ou mais dos seguintes meios: eletronicamente pelo portal de serviços, e-mail, telefone, Telegram e/ou outros aplicativos de Instant Messenger (IM).

3.7.2.3.7. Fornecer um relatório semanal sobre ameaças bloqueadas de baixa a média prioridade com recomendações conforme necessário para manter uma base de conhecimento sobre as ameaças conhecidas e procedimentos adotados.

3.7.2.3.8 Produzir relatórios e dashboards contendo as principais detecções e eventos de segurança.

3.7.2.3.9 Liberar avisos à medida que novas informações são obtidas sobre ameaças novas ou inovadoras. Tais avisos não precisam ser especificamente focados no ambiente da Contratante, podendo ser de natureza ampla e genérica.

3.7.2.3.10 Fornecer um relatório semanal sobre ameaças bloqueadas de baixa a média prioridade com recomendações conforme necessário.

3.7.2.3.11 Fazer recomendações a Contratante quanto a quaisquer ações de resposta a serem executadas nos terminais em resposta a uma ameaça identificada.

3.8. Serviços de treinamento nas soluções (itens 8, 9, 10, 11, 12 e 13)

Conforme disposto no subtópico 5.12 do Termo de Referência.

4. ASSINATURA DOS MEMBROS DA EQUIPE RESPONSÁVEL PELA ELABORAÇÃO

Fabio Ivo Analista de Rede/Telecom ID 51430320	Manuelito de Sousa Reis Júnior Gerente de Riscos e Ameaças ID 4406953-7

Rio de Janeiro, 23 de novembro de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/11/2023, às 11:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 24/11/2023, às 11:15, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **63878350** e o código CRC **A336FA02**.

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

Governo do Estado do Rio de Janeiro

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

Diretoria de Segurança da Informação

ANEXO II DO TERMO DE REFERÊNCIA

ROTEIRO PARA O TESTE DE BANCADA

Será realizado o teste de bancada com o objetivo de que seja verificado o atendimento dos requisitos funcionais considerados prioritários pelo PRODERJ, referente à proposta ofertada pela licitante arrematante. O roteiro do teste de bancada, nos termos que seguem abaixo, exigirá da licitante arrematante a comprovação de que sua solução atende as especificações de maior relevância aqui elencadas. As especificações selecionadas neste anexo representam as características de maior impacto em relação a solução como um todo, e levam em consideração os aspectos técnicos que permitem comprovação em ambiente de teste, haja vista que determinados recursos/características/funcionalidades possuem restrições de comprovação quando a solução ainda não está completamente implementada.

CARACTERÍSTICAS E FUNCIONALIDADES A SEREM COMPROVADAS:

1. SOBRE A SOLUÇÃO EDR PARA ESTAÇÕES DE TRABALHO (ITEM 1)

Solução EDR para estações de trabalho (Item 1)			OBSERVAÇÃO	REQUISITO APROVADO (SIM/NÃO)
ITEM Nº	REF. ANEXO I	DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO		
1	3.1.2.1.	A solução Antivírus_EDR do item 1 deverá ser gerenciada através de painel centralizado, disponibilizado na nuvem da Contratada ou do Fabricante da Solução, onde o acesso ocorrerá de maneira criptografada (SSL/TLS).	Contexto do requisito: "Administração e Gerência"	
2	3.1.2.3.	A console de gerenciamento centralizado deve permitir a integração e correlação de eventos entre todos os componentes da solução ofertada;	Contexto do requisito: "Administração e Gerência"	
3	3.1.2.7.	A Solução deve gerar relatório de compliance com informações de máquinas que nunca realizaram scan, políticas inconsistentes entre servidor/agente e componentes desatualizados;	Contexto do requisito: "Administração e Gerência"	
4	3.1.2.9.	A solução deve permitir níveis de administração da console por usuários ou grupos de usuários;	Contexto do requisito: "Administração e Gerência"	
5	3.1.2.24.	Deve permitir a escolha do intervalo de tempo necessário para que uma estação seja considerada off-line;	Contexto do requisito: "Administração e Gerência"	
6	3.1.2.29.	Deve permitir pesquisas personalizadas para a consulta de eventos (logs) através de categorias;	Contexto do requisito: "Administração e Gerência"	
7	3.1.2.32.	Deve de permitir a criação de políticas de segurança personalizadas;	Contexto do requisito: "Administração e Gerência"	

8	3.1.2.34.	Deve permitir a criação de múltiplos painéis (dashboards) personalizáveis, compostos por blocos de informações (widgets), visualizados através de gráficos ou tabelas;	Contexto do requisito: "Administração e Gerência"	
9	3.1.2.38.	Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;	Contexto do requisito: "Administração e Gerência"	
10	3.1.2.45.	Deve permitir a desinstalação através da console de gerenciamento da solução;	Contexto do requisito: "Administração e Gerência"	
11	3.1.2.48.	Deve permitir a deleção dos arquivos quarentenados;	Contexto do requisito: "Administração e Gerência"	
12	3.1.3.1.	A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações, Controle de dispositivos e EDR (Endpoint Detection and Response) em um único agente;	Contexto do requisito: "Funcionalidades de Proteção a Endpoints"	
13	3.1.3.2.15.	Deve possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;	Contexto do requisito: "Funcionalidades de Proteção a Endpoints"	
14	3.1.3.2.16.	Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no sistema;	Contexto do requisito: "Funcionalidades de Proteção a Endpoints"	
15	3.1.3.3.5.	Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;	Contexto do requisito: "Funcionalidades de proteção contra URL's Maliciosas"	
16	3.1.3.4.3.	Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;	Contexto do requisito: "Funcionalidades de Controle de Dispositivos"	
17	3.1.3.5.7.	A solução deverá possibilitar a criação de regras de bloqueio ou liberação, utilizando parâmetros como por exemplo: endereço IP, endereço MAC, portas de comunicação, protocolo, etc;	Contexto do requisito: "Funcionalidades de Firewall"	
18	3.1.3.5.10.	O firewall deverá permitir liberar ou apenas logar eventos;	Contexto do requisito: "Funcionalidades de Firewall"	

19	3.1.3.6.3.	A solução deve ter a capacidade de detectar uma conexão maliciosa e bloqueá-la;	Contexto do requisito: "Funcionalidades de IPS para Estações de Trabalho"	
20	3.1.3.7.1.	As regras de controle de aplicação devem permitir as seguintes ações: liberar e bloquear;	Contexto do requisito: "Funcionalidade de controle de aplicações"	
21	3.1.3.7.9.	O modulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionadas para bloqueio e monitoramento.	Contexto do requisito: "Funcionalidade de controle de aplicações"	

2. **SOBRE A SOLUÇÃO EDR PARA SERVIDORES (ITEM 2)**

Solução EDR para Servidores (Item 2)			**OBSERVAÇÃO**	**REQUISITO APROVADO? (SIM/NÃO)**
ITEM Nº	**REF. ANEXO I**	**DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO**		
	3.2.1.	A solução deverá ser compatível com no mínimo os sistemas operacionais:		
22	3.2.1.1.4.	Windows Server 2019 (64-bit);	Contexto do requisito: compatibilidade do agente	
23	3.2.1.2.1.	Red Hat Enterprise Linux 8 (64 bits);	Contexto do requisito: compatibilidade do agente	
24	3.2.10.17.	A solução deve ser capaz de tentar forçar a comunicação com o agente.	Contexto do requisito: "Proteção antimalware"	
25	3.2.11.1.	Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;	Contexto do requisito: Proteção contra URL's maliciosas"	
26	3.2.11.6.	A solução deve permitir que o administrador reclassifique uma URL para evitar falsos positivos.	Contexto do requisito: Proteção contra URL's maliciosas"	
27	3.2.13.4.	A solução deve ter a capacidade de definir regras distintas para interfaces de rede distintas;	Contexto do requisito: "Funcionalidades de Firewall"	
28	3.2.13.5.	A solução deverá ser capaz de identificar e possibilitar o bloqueio a endereços IP que estejam realizando escaneamento de rede, portas, protocolos e outras formas de reconhecimento;	Contexto do requisito: "Funcionalidades de Firewall"	

29	3.2.13.11.	O firewall deverá permitir liberar ou apenas logar eventos;	Contexto do requisito: "Funcionalidades de Firewall"	
30	3.2.14.3.	A solução deve ter a capacidade de detectar uma conexão maliciosa e bloqueá-la;	Contexto do requisito: "Funcionalidades de IPS"	
31	3.2.14.6.	Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);	Contexto do requisito: "Funcionalidades de IPS"	
32	3.2.15.6.	Monitoração de Status - Visualização do status dos hosts gerenciados, incluindo a realização de healthcheks.	Contexto do requisito: "Funcionalidade de controle de aplicações"	
33	3.2.16.6.	Deverá monitorar mudanças efetuadas no registro do Windows;	Contexto do requisito: "Monitoramento de Integridae e Rastreabilidade"	
34	3.2.16.9.	Deverá realizar auditoria no sistema operacional e aplicações (agendada e manual), para destacar e atribuir automaticamente a regra relevante para monitoramento de integridade de acordo com o resultado dessa auditoria;	Contexto do requisito: "Monitoramento de Integridae e Rastreabilidade"	
35	3.2.16.16.	Deverá ser possível gerar relatório de todas as modificações que ocorram nos objetos monitorados;	Contexto do requisito: "Monitoramento de Integridae e Rastreabilidade"	
	3.2.18.2.	Deverá possuir as seguintes configurações ou semelhante:		
36	3.2.18.2.1.	Bloqueio: possibilitando o bloqueio de aplicações, impedindo a execução de todos os softwares novos ou alterados, a menos que sejam expressamente permitidos;	Contexto do requisito: "Funcionalidade de controle de aplicações"	
37	3.2.18.2.2.	Permitido: possibilitando que aplicações sejam executadas por padrão, a menos que que sejam expressamente bloqueadas;	Contexto do requisito: "Funcionalidade de controle de aplicações"	
38	3.2.19.1.	A solução deverá ser gerenciada por console Web, devendo suportar certificado digital para gerenciamento;	Contexto do requisito: "Gerenciamento"	
39	3.2.19.11.	Deverá armazenar os eventos de auditoria envolvendo todos os eventos e ações realizadas na console de gerenciamento;	Contexto do requisito: "Gerenciamento"	

40	3.2.19.13.	A console deverá ter a capacidade de se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução, com permissões customizadas pela própria solução;	Contexto do requisito: "Gerenciamento"	
41	3.2.19.18.	Deverá ser possível criar políticas de forma global para todas os servidores, por perfis e individualmente para cada host;	Contexto do requisito: "Gerenciamento"	

3. **SOBRE A SOLUÇÃO XDR (ITEM 6)**

Solução XDR (Item 6)			OBSERVAÇÃO	REQUISITO APROVADO? (SIM/NÃO)
ITEM Nº	REF. ANEXO I	DESCRIÇÃO DO ITEM PARA COMPROVAÇÃO		
42	3.6.5.	Deve permitir alterar os status de cada evento;	Contexto do requisito: "Características Gerais"	
43	3.6.12.6.	Deve enviar alertas de notificação por email;	Contexto do requisito: "Investigação de Incidentes"	
44	3.6.13.1.	Análise de rede para repetição das comunicações e visualização das comunicações e tráfego lateral.	Contexto do requisito: "Visualização das ações de ameaça"	
45	3.6.13.16.	A solução deve fornecer a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;	Contexto do requisito: "Visualização das ações de ameaça"	
46	3.6.13.20.	Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;	Contexto do requisito: "Visualização das ações de ameaça"	
47	3.6.13.31.	Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;	Contexto do requisito: "Visualização das ações de ameaça"	
48	3.6.13.46.	Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;	Contexto do requisito: "Visualização das ações de ameaça"	
49	3.6.13.47.	Restaurar a conectividade da estação de trabalho com a rede;	Contexto do requisito: "Visualização das ações de ameaça"	
50	3.6.13.48.	Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;	Contexto do requisito: "Visualização das ações de ameaça"	

Rio de Janeiro, 23 de novembro de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/11/2023, às 11:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 24/11/2023, às 11:16, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

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

Governo do Estado do Rio de Janeiro

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

Diretoria de Segurança da Informação

ANEXO III DO TERMO DE REFERÊNCIA

MODELO DE ORDEM DE SERVIÇO

1 - IDENTIFICAÇÃO DA ORDEM DE SERVIÇO			
N°da OS:	Data de Emissao:	N° do Contrato:	Data do Contrato: Extrato DOERJ:

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

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

4 – INSTRUÇÕES COMPLEMENTARES

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

Rio de Janeiro, 23 de novembro de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/11/2023, às 11:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 24/11/2023, às 11:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

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

Governo do Estado do Rio de Janeiro

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

Diretoria de Segurança da Informação

ANEXO IV DO TERMO DE REFERÊNCIA

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

ANEXO XXX - DO CONTRATO

MODELO DE TERMO DE CONFIDENCIALIDADE E SIGILO

O _____, sediado em _____, CNPJ n.°_____, doravante denominado CONTRATANTE, e, de outro lado, a _____, sediada em _____ , CNPJ n.°_____, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação do CONTRATANTE; Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, de dados pessoais de agentes públicos e de cidadãos, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei nº 12.527, de 18/11/2011 e Decreto Estadual n° 46.475/2018, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo, além da Lei nº 13.709, de 14/08/2018 que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais (Lei Geral de Proteção de Dados Pessoais - LGPD).

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto, reservado, dado pessoal e dado pessoal sensível. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio do CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados e contratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga

a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

A vigência deste Termo independe do prazo de vigência do contrato assinado.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro - Havendo necessidade legal devido a Programas de Governo, a CONTRATADA assume o compromisso de assinar Termo de Sigilo (ou equivalente) adicional relacionado ao Programa, prevalecendo as cláusulas mais restritivas em benefício do CONTRATANTE.

Parágrafo Quarto – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – O CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pelo CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

O CONTRATANTE elege o foro da _____ , onde está localizada a sede do CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

_____, _____ de _____ de 20____

De Acordo.

CONTRATANTE

CONTRATADA

Matrícula: _____

TESTEMUNHAS

Testemunha 1 _____

Testemunha 2 _____

Rio de Janeiro, 23 de novembro de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/11/2023, às 11:05, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 24/11/2023, às 11:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **63879241** e o código CRC **78282ED8**.

Referência: Processo nº SEI-150016/001346/2022 SEI nº 63879241

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

Governo do Estado do Rio de Janeiro

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

Diretoria de Segurança da Informação

ANEXO V DO TERMO DE REFERÊNCIA

MODELO DE PLANILHA DE CUSTOS

(PAPEL TIMBRADO DA EMPRESA)

Processo SEI Nº_____

Pregão Nº ____/____

Empresa:

OBJETO: Contratação de empresa de Tecnologia da Informação para o fornecimento de solução de segurança para proteção de dispositivos finais (antivírus), aplicações em nuvem, servidores de e-mail e detecção/resposta unificada a eventos de segurança que envolvam a solução, contemplando o treinamento para operacionalização e o suporte técnico para as soluções contratadas.

Item	ID SIGA	Descrição	Métrica	Quantidade	Valor Unitário (R$)	Valor Total (R$)
01	181940	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para ESTAÇÕES DE TRABALHO, incluído o suporte técnico (por 36 meses)	unidade			
02	181941	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para SERVIDORES, incluído o suporte técnico (por 36 meses)	unidade			
03	181942	Subscrição de licenças de uso para solução de proteção a dispositivos finais (EDR) - para DISPOSITIVOS MÓVEIS, incluído o suporte técnico (por 36 meses)	unidade			

04	181943	Subscrição de licenças de uso para solução de proteção a aplicações em nuvem, incluído o suporte técnico (por 36 meses)	unidade (usuário)			
05	181944	Subscrição de licenças de uso para solução de Proteção a servidores de e-mail, incluído o suporte técnico (por 36 meses)	unidade (usuário)			
06	181945	Subscrição de licenças de uso para solução de visibilidade, detecção, investigação e alertas de incidentes (XDR), incluído o suporte (36 meses)	unidade			
07	181952	Serviço gerenciado de detecção e resposta (MDR) (pelo período de 36 meses)	serviço			
08	181946	Serviço de treinamento na solução EDR para estações de trabalho	vaga / aluno			
09	181947	Serviço de treinamento na solução EDR para servidores	vaga / aluno			
10	181948	Serviço de treinamento na solução EDR para dispositivos móveis	vaga / aluno			
11	181949	Serviço de treinamento na solução de proteção a aplicações em nuvem	vaga / aluno			
12	181950	Serviço de treinamento na solução de proteção a servidores de e-mail	vaga / aluno			
13	181951	Serviço de treinamento na solução XDR	vaga / aluno			
Valor Total a pagamento:						

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

Rio de Janeiro, 23 de novembro de 2023

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 24/11/2023, às 11:06, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

Documento assinado eletronicamente por **Fabio Ivo**, **Assistente**, em 24/11/2023, às 11:17, conforme horário oficial de Brasília, com fundamento nos art. 28º e 29º do Decreto nº 48.209, de 19 de setembro de 2022.

A autenticidade deste documento pode ser conferida no site http://sei.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **63880427** e o código CRC **1702B60E**.

Referência: Processo nº SEI-150016/001346/2022 SEI nº 63880427

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