TERMO DE REFERÊNCIA

ANEXO I DO EDITAL
CONTRATAÇÃO DE SOLUÇÃO DE SEGURANÇA PARA ESTAÇÕES DE TRABALHO, DISPOSITIVOS MÓVEIS E SERVIDORES

(ANTIVÍRUS)

1. PROPÓSITO

I - O presente Termo de Referência tem por objetivo descrever a contratação de serviços de subscrição de licenças de uso para solução antivírus, contemplando implementação, configuração, suporte, garantia e transferência de conhecimento para proteção de estações de trabalho, dispositivos móveis, servidores Windows e Linux, por empresa, em conformidade com a 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 o Decreto Estadual nº 46.642/2019 (Regulamenta a fase preparatória das contratações no âmbito do Estado do Rio de Janeiro).

II - O PRODERJ é o órgão responsável pelo procedimento para fins deste Registro de Preços, nos termos do art. 5º, XVII, Decreto nº 47.278/2020.

III - Na licitação para registro de preços não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento hábil, conforme disposição do §2º, art. 10, do Decreto nº 46.751/2019.

1.1. Justificativa da contratação

1.1.1. O Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro - PRODERJ, nos termos do art. 5º do Decreto nº 47.278/2020, é o Órgão Gestor do Sistema Estadual de Tecnologia da Informação e Comunicação - SETIC, composto pelo conjunto de recursos humanos, tecnológicos e de equipamentos voltados para o estabelecimento e a implementação de políticas para a informação e a comunicação pública.

1.1.2. O PRODERJ 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.

1.1.3. Ademais, o Decreto nº 46.751/2019, regulamentador do Sistema de Registro de Preços no Estado do Rio de Janeiro, em seu §2º, do art. 4º, atribui ao PRODERJ a competência para 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.

1.1.4. Nos tempos atuais, quase que a totalidade das políticas e dos serviços públicos são ofertados, direta ou indiretamente, através de sistemas tecnológicos. Tal realidade representa acesso rápido à informação, bem como atendimento menos burocrático às demandas da sociedade, notadamente dos cidadãos.

1.1.5. Contudo, o uso de tais sistemas, associado à contínua evolução dos serviços públicos traz riscos ao Governo Estadual, enquanto prestador de tais serviços e guardião de informações importantes, sobretudo dados pessoais dos cidadãos fluminenses, razão pela qual deve se precaver para a manutenção do funcionamento ininterrupto dos seus serviços, de forma segura.

1.1.6. A segurança cibernética é, portanto, fundamental para o perfeito funcionamento do Estado, cuja responsabilidade inclui registros, cadastros, integrações, acessos, inclusões, guardas e tratamentos de informações públicas e privadas dentro do ambiente tecnológico, o que torna o PRODERJ, bem como os diversos órgãos da Administração, alvos constantes de cyber ataques.

1.1.7. O aumento do uso de dispositivos móveis e de dispositivos de armazenamento através de interfaces externas como a USB, e 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 da informação dentro dessas redes locais, sendo necessário que, cada estação de trabalho ou servidor que esteja conectado a 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 dos softwares de antivírus em estações de trabalho.

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

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

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

1.1.11. 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 rede mundial ou através de engenharia social, com tamanha sofisticação que essas ameaças conseguem evadir as defesas convencionais e permanecerem ocultas enquanto roubam dados corporativos.

1.1.12. Para detectar essas intrusões criminais, analistas e especialistas em segurança da informação recomendam que as organizações implementem proteção avançada contra ameaças como parte de uma estratégia de monitoramento de segurança.

1.1.13. Há, por fim, a necessidade de padronização deste tipo de solução corporativa de proteção para todos os Órgãos do Estado do Rio de Janeiro, pois, através desta padronização, será possível o PRODERJ, como gestor de TIC, ter maior visibilidade da segurança de todo de todo parque computacional do Governo do Estado, possibilitando uma atuação mais efetiva nos casos de incidentes e na gestão da segurança da informação como um todo.

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

1.2. Instrumentos de planejamento

1.2.1. A contratação almejada encontra alinhamento estratégico com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) do PRODERJ para o

período de 2018-2021, conforme descrito em sua página 21:

Objetivo Estratégico 7 - Promover o processo de Segurança da Informação e Comunicações: 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.

1.2.2. A contratação almejada também encontra alinhamento estratégico com o Plano Pluri-Anual (PPA) 2020-2023, registrada com o código de ação nº 1293 e código do produto nº 6884.

1.2.3. Pelas considerações e justificativas acima já elencadas e cientes de que o conjunto de investidas de ações danosas, sequestros de dados e atividades maliciosas que diariamente atentam contra a segurança de ativos, seja por e-mails, por exploração de vulnerabilidades em nossos sistemas, por ataques diretos na infraestrutura tecnológica, oriundos de atores nacionais e internacionais, entendemos indispensável a utilização de uma ferramenta atual e robusta de segurança corporativa de estações de trabalho, dispositivos móveis e servidores, a fim de contribuir com o alcance dos objetivos estratégicos definidos no PDTIC e no PPA.

1.3. Objetivo da contratação

1.3.1. Melhorar as ações de segurança da informação no âmbito da Administração Pública;

1.3.2. Implementar mecanismos sofisticados para proteção contra o vazamento de informações sensíveis;

1.3.3. Aumentar o grau de confidencialidade da segurança da informação;

1.3.4. Elevar a integridade e segurança de dados;

1.3.5. Assegurar o provimento de Infraestrutura de TI segura e adequada para que as áreas finalísticas do órgão licitante continuem operacionais;

1.3.6. Contribuir para a garantia da disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;

1.3.7. Robustecer e ampliar os quesitos de segurança das estações de trabalho, servidores Windows e Linux e dispositivos móveis contra ameaças cibernéticas, melhorando a atual gestão de incidentes de segurança e ainda padronizando e homogeneizando as soluções e ferramentas para um ganho em escala tanto no campo financeiro quanto no campo técnico, na medida em que:

- Aumentar a segurança nos acessos aos sistemas;
- Garantir a integridade das informações disponibilizadas;
- Prevenir contra fraudes e ameaças digitais;
- Possuir maior capacidade de identificar acessos indevidos com credenciais válidas;
- Gerar dados e informações para maior eficiência das equipes de tratamento e resposta a incidentes;
- Der maior agilidade e consequentemente efetividade no bloqueio de acessos indevidos;
- Atuar no incremento da segurança de seus sistemas sem interferência nas regras de negócio;
- Der maior aderência com a legislação e orientações relacionadas à proteção de dados pessoais e a segurança das informações;
- Realizar o registro de informações úteis à auditoria de incidentes de segurança; e
- Criar indicadores de uso dos sistemas associados à credencial de acesso (hora/local/área).

1.3.8. Cumprir as disposições da Lei Nº 4.480/2004, em que o PRODERJ:

- é o Órgão responsável por "administrar, manter e operar a infraestrutura de comunicações, representada pela Rede Governo, atuando como ponto focal de convergência das diversas redes locais dos Órgãos do Estado, oferecendo conectividade global a todas as áreas de Tecnologia de Informação e Comunicação do Governo, incluindo os equipamentos corporativos centralizados", para a Administração Pública Estadual;
- deve projetar, desenvolver, sediar, manter e operar bases de dados corporativas operacionais e de suporte à decisão, de sistemas sediados no Centro de Tecnologia da Informação e Comunicação do Estado do Rio de Janeiro, e de outros geridos pelos Órgãos da Administração Direta e Indireta cuja integração seja necessária para uso corporativo do Governo do Estado;

1.3.9. Atender aos decretos 46.751/2019 e 47.278/2020, que determinam ao PRODERJ conduzir e disponibilizar as atas de registro de preços e contratos corporativos para suprir itens relativos à TIC aos Órgãos e entidades do Governo do Estado.

1.3.10. Promover o compliance com a legislação vigente, notadamente quanto à da Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), que estabelece no capítulo IV - DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO diversas regras que deverão obrigatoriamente ser cumpridas pelo PRODERJ e demais órgãos da administração pública estadual, dos quais destacamos:

- "Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.".
- "Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.".
- "Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, às entidades do Poder Público, a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito e a natureza dos dados e demais detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.".
- "Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação."
- "Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público."

1.4. Modelo de licitação e demonstração do critério para aceitabilidade de preços.

1.4.1. A licitação ocorrerá em modalidade pregão, em sua forma eletrônica, no tipo menor preço global por lote.

1.4.2. O critério de aceitabilidade de preços e escolha da melhor proposta terá como parâmetro o "preço máximo total", aferido em pesquisa de mercado e informado no Edital.

2. DESCRIÇÃO DO OBJETO

2.1. Definição do Objeto

2.1.1. Registro de Preços para 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, conforme especificações e condições constantes neste Termo de Referência e seus anexos.

2.2. Identificação dos itens, quantidades e unidades.

Lote 1

Código do item	ID	Descrição	Unidade de fornecimento	Quantidade Estimada
1	167761	Descrição: Subscrição de licenças de uso para solução Antivírus (Estações de trabalho). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	UN	46.286
2	167762	Descrição: Subscrição de licenças de uso para solução Antivírus (Servidores). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	UN	2.040
3	167764	Serviço de treinamento para solução antivírus (Estações de trabalho e Servidores)	Turma	81
4	167766	Serviço de suporte técnico para solução antivírus (estações de trabalho e servidores), remoto 24x7. Origem: Pessoa jurídica, Fornecimento: 36 meses	UN	20.027

Lote 2

Código do item	ID	Descrição	Unidade de fornecimento	Quantidade Estimada
1	167763	Descrição: Subscrição de licenças de uso para solução Antivírus (Dispositivos móveis). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	UN	777
2	167765	Serviço de treinamento para solução antivírus (Dispositivos móveis).	Turma	58
3	167767	Serviço de suporte técnico para solução antivírus (dispositivos móveis), remoto 24x7. Origem: Pessoa jurídica, Fornecimento: 36 meses	UN	49

2.2.1. Quantidades estimadas para cada órgão participante

Orgão participante	Lote 1				Lote 2		
	Id 167761	Id 167762	Id 167764	Id 167766	Id 167763	Id 167765	Id 167767
AGENERSA - AG REGUL ENERGIA E SANEAMENTO DO EST RJ	100	2	3	0	0	0	0
CENTRAL - COMP EST DE ENGENH DE TRANSPORTES E LOGÍSTICA	200	10	5	200	30	30	30
CEPERJ - FUND CENTRO EST. ESTAT. PESQ. SERV RJ	200	3	4	4	20	4	0
CGE - CONTROLADORIA GERAL DO ESTADO DO RJ	350	30	0	0	0	3	0
CODERTE - COMP DE DESENV RODOV E TERMINAIS DO EST DO RJ	101	0	0	0	0	0	0
CODIN - COMP DE DESENV INDUSTRIAL DO ESTADO DO RJ	100	30	1	1	0	0	0
DEGASE - Dep Geral de Ações Socioeducativas	900	10	20	10	90	8	0

DER-RJ - FUND DEP ESTRADAS DE RODAGEM DO ESTADO DO RJ	500	7	2	1	0	0	0
DETRAN - DEPARTAMENTO DE TRÂNSITO DO ESTADO DO RJ	6000	300	1	1	500	1	1
EMOP - EMPRESA DE OBRAS PÚBLICAS DO ESTADO DO RJ	350	5	0	400	0	0	0
FAPERJ - FUNDAÇÃO C.C.F. DE AMPARO À PESQUISA DO ERJ	150	15	10	10	0	0	0
FLXIII - FUNDAÇÃO LEÃO XIII	246	4	2	250	0	0	0
FTMRJ - FUNDAÇÃO TEATRO MUNICIPAL DO RIO DE JANEIRO	0	2	0	0	0	0	0
FUNARJ - FUND ANITA MANTUANO DE ARTES DO EST DO RJ	150	5	0	0	0	0	0
GSI - Gabinete de Segurança Institucional do Governo do Estado do Rio de Janeiro	125	10	0	0	0	0	0
- IEEA - INST ESTADUAL DE ENGENHARIA E ARQUITETURA	50	10	5	50	0	0	0
INEA - INSTITUTO ESTADUAL DO AMBIENTE	1080	110	4	1	0	0	0
IPEM-RJ - INSTITUTO DE PESOS E MEDIDAS DO ESTADO DO RJ	230	20	1	1	30	1	1
ITERJ - INSTIT DE TERRAS E CARTOGRAFIA DO EST DO RJ	150	1	1	0	7	1	7
LOTERJ - LOTERIA DO ESTADO DO RIO DE JANEIRO	80	4	0	0	0	0	0
PROCON RJ - Proteção e Defesa do Consumidor	200	4	0	0	0	0	0
PRODERJ - CENTRO DE TECN DE INFORMAÇÃO E COMUN DO ERJ	375	763	5	5	100	10	10
RIO METRÓPOLE - Instituto Rio Metrópole	50	2	0	0	0	0	0
RIOPREVIDÊNCIA - FUNDO UNICO DE PREVIDENCIA DO ERJ	720	89	2	806	0	0	0
SECC - Secretaria de Estado da Casa Civil (Antiga SEGOV)	791	4	8	791	0	0	0
SECEC - Sec de Estado de Cultura e Econ Criativa	450	55	2	505	0	0	0
SEDEERI - SEC DE EST DESENV ECONÔM ENER REL INTERNACIONAIS (ANTIGA SEDEIS)	150	4	1	0	0	0	0
SEEDUC - SECRETARIA DE ESTADO DE EDUCAÇÃO	16.988	0	1	16.988	0	0	0
SEPM - Secretaria de Estado de Polícia Militar	13.000	407	2	2	0	0	0
SES - SECRET ESTADO SAÚDE	2300	130	0	0	0	0	0
SETRAB - SECRETARIA DE ESTADO DO TRABALHO E RENDA	200	4	1	1	0	0	0
TOTAL	**46.286**	**2.040**	**81**	**20.027**	**777**	**58**	**49**

2.2.2. Os endereços de entrega para cada órgão constarão no Edital.

2.2.3. Quantidades estimadas para adesão por órgãos não participantes

2.2.3.1. O quantitativo decorrente das adesões à Ata de Registro de Preços decorrente deste certame, não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata para o órgão gerenciador e órgãos participantes (tabelas dos lotes 1 e 2, do item 2.2.), independente do número de órgãos não participantes que aderirem.

2.2.3.2. À Ata de Registro de Preços decorrente deste certame poderão aderir os órgãos ou entidades, sociedades de economia mista e empresas públicas do Estado, que não tenham participado da licitação, bem como as entidades municipais, distritais, de outros estados e federais, resguardadas as disposições contrárias de cada ente, mediante anuência do órgão gerenciador e da empresa beneficiária da ata, e conforme as exigências do art. 26 e seus parágrafos, do Decreto nª 46.751/19.

2.3. Definição da natureza do Objeto

2.3.1. Trata-se de serviço comum a ser contratado mediante licitação, na modalidade pregão, em sua forma eletrônica, para escolha de proposta do tipo menor preço global por lote.

3. DESCRIÇÃO DA SOLUÇÃO

I - As especificações técnicas e a descrição dos serviços que compõem a solução estão descritas no Anexo I deste Termo de Referência.

II - Para fins de cumprimento do inciso XIII, do art. 11, do Decreto nº 46.642/2019, quanto aos itens 3 e 4 do Lote 1 e itens 2 e 3 do Lote 2, que correspondem respectivamente aos itens 2.3, 2.4, 3.2 e 3.3 do Anexo I – Especificações Técnicas, considerar:

- 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.
- 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.

3.1. Forma de execução

3.1.1. As especificações técnicas e outros detalhes relativos à entrega do objeto estão descritas no Anexo I deste Termo de Referência.

3.1.2. Regime de Execução

O regime de execução indireta do objeto é o previsto no art. 10, II, "a", da Lei nº 8.666/93, empreitada por preço global.

3.2. Duração do contrato

3.2.1. O prazo de vigência do contrato será de 36 (trinta e seis) meses, contados a partir da data de assinatura do seu termo pelas partes;

3.2.2. O prazo contratual poderá ser prorrogado por 12 (doze) meses, observando-se o limite previsto no art. 57, IV, da Lei nº 8.666/93 e 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.

3.2.3. A CONTRATADA sujeitar-se-á aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei no 8.666/93.

3.3. Reajuste de preços

3.3.1. Os valores constantes da Ata de Registro de Preços não sofrerão reajuste, exceto nos casos previstos no art. 18, do Decreto nº 7.892 de 23 de Janeiro de 2013 e nos art. 21 e art. 22, do Decreto 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.

3.3.2. Os contratos gerados a partir da Ata de Registro de Preços poderão, em uma eventual prorrogação, ter os seus preços reajustados, a cada 12 (doze) meses contados da data limite da apresentação da proposta, aplicando-se a variação do Índice de Preços ao Consumidor Amplo – IPCA, ou outro que o venha substituir, nos termos do art. 40, inciso XI, da Lei nº 8.666/1993 e do art. 19, inciso XXII, da IN nº 02/2008 SLTI/MP.

3.4. Garantia

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

3.4.2. 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.

3.4.3. A garantia prestada não poderá se vincular a outras contratações, salvo após sua liberação.

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

3.4.5. O item 3.4. será detalhado no edital.

3.5. Critérios e práticas de sustentabilidade

3.5.1. O fornecedor deverá obedecer aos critérios estabelecidos no art. 2º Decreto estadual 43.629/2012.

3.6. Possibilidade de subcontratação

3.6.1. É vedada a subcontratação total ou parcial do objeto, tendo em vista que os itens a serem contratados são interdependentes e formam uma ou várias soluções.

3.6.2. O suporte técnico do fabricante não caracteriza subcontratação.

3.7. Possibilidade de participação de Consórcio

3.7.1. Não será permitida a participação de empresas que estiverem reunidas em consórcio, qualquer que seja sua forma de constituição, dadas as características específicas dos itens que serão fornecidos, que não pressupõem multiplicidade de atividades empresariais distintas (heterogeneidade de atividades empresariais).

3.7.2. A ausência de consórcio ou cooperativas não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital. Nestes casos, a Administração, com vistas a aumentar o número de participantes, admite a formação de consórcio.

3.7.3. Tendo em vista que é prerrogativa do Poder Público, na condição de contratante, a escolha da participação, ou não, de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme se depreende da literalidade do texto da Lei nº 8.666/93, que em seu artigo 33 que atribui à Administração a prerrogativa de admissão de consórcios em licitações por ela promovidas, pelos motivos já expostos, conclui-se que a vedação de constituição de empresas em consórcio, para o caso concreto, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

3.7.4. Ademais, essa vedação visa exatamente afastar a restrição à competição, na medida que a reunião de empresas que, individualmente, poderiam prestar os serviços, reduziria o número de licitantes e poderia, eventualmente, proporcionar a formação de conluios/carteis para manipular os preços nas licitações.

3.8. Possibilidade de participação de Cooperativa

Será admitida a participação de cooperativas pertencentes ao ramo de atividade relacionado ao objeto deste certame, enquadradas no art. 34, da Lei nº 11.488/2007, desde que atendidos os requisitos e condições do Edital e do Termo de Referência, resguardadas, as disposições dos art. 42 a 45 da Lei Complementar n.º 123/2006.

3.9. Incidência do Programa de Integridade

3.9.1. Será exigida da empresa contratada a efetivação do Programa de Integridade, nos termos da Lei nº 7.753/2017, uma vez que o objeto se enquadra no art. 1º do referido diploma.

3.9.2. A implantação do Programa de Integridade no âmbito da empresa contratada dar-se-á no prazo de 180 (cento e oitenta) dias corridos, a partir da data de celebração do contrato.

3.9.3. A empresa que possuir o Programa de Integridade implantado deverá apresentar no momento da contratação declaração informando a sua existência.

3.10. Responsabilidades das partes

3.10.1. **Obrigações da contratante**

3.10.1.1. Efetuar os pagamentos devidos ao Fornecedor, de acordo com as condições estabelecidas nesta Ata de Registro de Preços.

3.10.1.2. Entregar ao Fornecedor documentos, informações e demais elementos que possuir e pertinentes à execução do presente contrato;

3.10.1.3. Exercer a fiscalização da execução do objeto;

3.10.1.4. Receber provisória e definitivamente o objeto, nas formas definidas no edital e no contrato, se houver.

3.10.2. **Obrigações da contratada**

3.10.2.1. Entregar o serviço, na quantidade, qualidade, local e prazos especificados, de acordo com as condições estabelecidas nesta Ata de Registro de Preços.

3.10.2.2. Entregar o objeto do contrato sem qualquer ônus para o **CONTRATANTE**, estando incluído no valor do pagamento todas e quaisquer despesas, tais como tributos, frete, seguro e descarregamento das mercadorias;

3.10.2.3. Manter em estoque um mínimo de bens necessários à execução do objeto do contrato;

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

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

3.10.2.6. 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** ou terceiros;

3.10.2.7. Não será admitida justificativa de atraso no fornecimento dos produtos adquiridos que tenha como fundamento o não cumprimento da sua entrega pelos fornecedores do licitante.

4. REQUISITOS MÍNIMOS PARA EXECUÇÃO

4.1. Qualificação Técnica

4.1.1- Para fins de comprovação de qualificação técnica, deverá(ão) ser apresentado(s) o(s) seguinte(s)documento(s):a) Atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado, que comprovem a aptidão de desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, na forma do artigo 30, § 4º, da Lei Federal nº 8.666/93 que indiquem nome, função, endereço de contato do(s) atestador(es), ou qualquer outro meio para eventual contato pelo ÓRGÃO GERENCIADOR.

4.2. Autorizações e Licenças Necessárias para a Execução do Objeto

4.2.1. As despesas e responsabilidade pela obtenção das autorizações quanto às permissões, aprovações e/ou licenças junto das autoridades governamentais federais, estaduais e municipais, agentes do serviço público, concessionárias de serviços públicos e quaisquer outros Órgãos/Entidades necessários, referentes à execução do objeto serão de responsabilidade da contratada.

4.2.2. Todas as autorizações e licenças referidas deverão ser mantidas durante todo o prazo da contratação, cabendo às empresas contratadas as renovações, substituições e demais providências relacionadas à sua atuação regular, competindo ao Órgão contratante a sua adequada fiscalização.

4.3. O contrato não contempla fornecimento de mão de obra residente.

5. GESTÃO E FISCALIZACÃO DO CONTRATO

5.1. Agentes que participarão da gestão do contrato

5.1.1. A gestão dos contratos oriundos de participação ou adesão a esta Ata, realizados por Órgãos ou entidades da Administração Pública do Estado do Rio de Janeiro, terá como gestor o PRODERJ e o Órgão participante.

5.1.2. O Órgão usuário do objeto contratado deverá nomear uma comissão de fiscalização composta por gestor, fiscais técnico, administrativo e requisitante que serão responsáveis por acompanhar e fiscalizar a execução do Contrato, devendo ser comunicadas ao Órgão gerenciador da Ata as eventuais ocorrências apuradas;

5.1.3. A comissão de fiscalização do contrato será responsável por atestar o pagamento das faturas mediante a conferência de que a contratada atendeu todos os requisitos deste Termo de Referência.

5.1.4. O Órgão participante ou aderente, que seja componente da Administração Pública do Estado do Rio de Janeiro, deverá enviar mensalmente ao PRODERJ relatório da solução adquirida, informando:

5.1.4.1. Quantidade de estações de trabalho, dispositivos móveis e servidores em uso, indicando:

1. Sistema Operacional,
2. Nome da Máquina,
3. Usuário,
4. Local onde está instalado,
5. Indicar se o endpoint está instalado e atualizado.

5.1.5. A contratada deverá designar e manter preposto nas suas próprias dependências, que deverá se reportar diretamente ao Fiscal do contrato, para acompanhar e se responsabilizar pela execução dos serviços, inclusive pela regularidade técnica e disciplinar da atuação da equipe técnica disponibilizada para os serviços.

5.2. Mecanismos de comunicação a serem estabelecidos

5.2.1. A troca de informações entre contratada e contratante será feita por meio do Gestor do contrato (por parte da contratante) e do Preposto (por parte da contratada), além dos seguintes meios:

1. Documento Oficial (Carta ou Ofício);
2. Correspondência eletrônica (e-mail);
3. Outros meios de comunicação definidos pela contratante.

5.3. Critérios de Medição

5.3.1. Estão estabelecidos Níveis de Serviço com a finalidade de aferir e avaliar diversos fatores relacionados aos serviços contratados, bem como orientar o pagamento por resultados obtidos.

5.3.2. A contratada deverá cumprir prazos máximos para respostas aos acionamentos, de acordo com o nível de severidade de cada chamado, conforme quadros abaixo:

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, remoto, E-mail, Fax ou Telefone	Início	30 minutos	45 minutos	60 minutos
	Término	2 horas	4 horas	8 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		

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

- 0,15% no valor da fatura do grupo correspondente do mês de referência, por demanda categorizada como “normal” não atendida;
- 0,25% no valor da fatura do grupo correspondente do mês de referência, por demanda categorizada como “crítico” não atendida;
- 0,50% no valor da fatura do grupo correspondente do mês de referência, por demanda categorizada como “urgente” não atendida;
- 3% no valor da fatura do grupo correspondente do mês de referência, por até 15 dias de não cumprimento do item categorizado como “Atualizações e aplicações diversas”;
- 5% no valor da fatura do grupo correspondente do mês de referência, por mais de 15 dias no mês corrente de não cumprimento do item categorizado como “Atualizações e aplicações diversas”;
- 2% no valor da fatura do grupo correspondente do mês de referência, por hora de indisponibilidade total, após o vencimento do prazo indicado na tabela;
- 1% no valor da fatura do grupo correspondente do mês de referência, por hora de indisponibilidade parcial, após o vencimento do prazo indicado na tabela;

5.3.4. Os descontos relativos à redução por não cumprimento do nível de serviço deverão ser aplicados na fatura do mês corrente;

5.3.5. 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;

5.3.6. Qualquer descumprimento do nível de serviço mínimo exigido poderá implicar na aplicação da Lei 8.666, Seção V (da inexecução e da rescisão dos contratos);

5.4. Recebimento provisório e definitivo do objeto

5.4.1. O recebimento provisório será realizado pela equipe de fiscalização, após a contratada entregar a documentação comprobatória do cumprimento da obrigação contratual. Esse recebimento será feito da seguinte forma:

5.4.1.1. A contratante realizará inspeção de todos os serviços executados, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a adequação dos serviços e constatar e relacionar os arremates, retoques e revisões finais que se fizerem necessários.

5.4.1.2. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

5.4.1.3. A Contratada fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no recebimento provisório.

5.4.1.4. Após o recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

5.4.1.5. Realizar a análise dos relatórios e de toda a documentação apresentada e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à contratada as respectivas correções;

5.4.1.6. Emitir Termo de Recebimento Definitivo, para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

5.4.1.7. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

5.5. Pagamento

5.5.1. O pagamento será realizado de maneira parcelada e mensal;

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

5.5.3. A nota fiscal deverá ser entregue acompanhada dos seguintes documentos:

5.5.3.1. Prova de regularidade para com as fazendas Federal, Estadual e Municipal; da regularidade relativa à Seguridade Social; do certificado de regularidade do FGTS e da Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho,

5.5.3.2. Cópia de todas as ordens de serviço concluídas no período;

5.5.3.3. Termo de Recebimento Definitivo assinado;

5.5.4. O contratado deverá emitir a Nota Fiscal Eletrônica – NF-e, consoante o Protocolo ICMS 42, de 3 de julho de 2009, com a redação conferida pelo Protocolo ICMS 85, de 9 de julho de 2010, e caso seu estabelecimento estiver localizado no Estado do Rio de Janeiro deverá observar a forma prescrita no § 1º, alíneas a, b, c e d, do art. 2º da Resolução SER 047/2003;

5.5.5. Caso se faça necessária a reapresentação de qualquer fatura por culpa do contratado, o prazo de 30 (trinta) dias ficará suspenso, prosseguindo a sua contagem a partir da data da respectiva reapresentação;

5.5.6. O Fornecedor será obrigado a reapresentar as certidões constantes no item 5.5.4. sempre que expirados os respectivos prazos de validade

1. Anexos do Termo de Referência

1.1. São partes integrantes deste Termo de Referência os seguintes Anexos:

- Anexo I – Especificações Técnicas dos Serviços;
- Anexo II – Termo de Recebimento Definitivo;
- Anexo III – Declaração de Não Utilização de Produtos Perigosos e Aderência aos Requisitos de Sustentabilidade Ambiental;
- Anexo IV - Modelo da Ordem de Serviço;
- Anexo V - Modelo de Planilha de Custos.

2. ASSINATURA DOS RESPONSÁVEIS PELA ELABORAÇÃO

Marcelo Soares Lintomen Assessor de Segurança da Informação 43541321	Rosana Alves de Andrade Analista de Sistemas 43474705

3. RATIFICAÇÃO DA AUTORIDADE COMPETENTE

Ratifico.

Flávio Sebastião Rodrigues da Silva
Vice-Presidente de Tecnologia
51098709

Rio de Janeiro, 09 setembro de 2021

Documento assinado eletronicamente por **Marcelo Soares Lintomen**, **Diretor**, em 10/09/2021, às 23:02, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 10/09/2021, às 23:07, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Rosana Alves de Andrade**, **Analista de Sistemas**, em 11/09/2021, às 09:54, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Referência: Processo nº SEI-120211/000548/2020	SEI nº 21955513

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

Criado por prmrei, versão 14 por prmrei em 10/09/2021 22:07:11.

ANEXO I DO TERMO DE REFERÊNCIA
ESPECIFICAÇÕES TÉCNICAS DA SOLUÇÃO

ÍNDICE

1. Descrição da Solução de Tecnologia da Informação

1.1. Características e Funcionalidades Gerais da Solução Antivírus

2. Funcionalidades Específicas da Solução Antivírus (LOTE 1)

2.1. Subscrição de licenças de uso para solução Antivírus (estações de trabalho)

2.2. Subscrição de licenças de uso para solução Antivírus (Servidores)

2.3. Serviço de treinamento para solução Antivírus (estações de trabalho e servidores)

2.4. Serviço de suporte técnico para solução Antivírus - remoto 24x7

3. Funcionalidades Específicas da Solução Antivírus (LOTE 2)

3.1. Subscrição de licenças de uso para solução Antivírus (Dispositivos móveis)

3.2. Serviço de treinamento para solução Antivírus (dispositivos móveis)

3.3. Serviço de suporte técnico para solução Antivírus - remoto 24x7

4. Demais requisitos da solução antivírus

4.1. Instalação e Configuração

4.2. Garantia do Fabricante

1. Descrição da Solução de Tecnologia da Informação

Lote 1

Código do item	ID	Descrição	Unidade de fornecimento	Quantidade estimada
1	167761	Descrição: Subscrição de licenças de uso para solução Antivírus (Estações de trabalho). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	UN	
2	167762	Descrição: Subscrição de licenças de uso para solução Antivírus (Servidores). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	UN	
3	167764	Serviço de treinamento para solução antivírus (Estações de trabalho e Servidores)	Turma	
4	167766	Serviço de suporte técnico para solução antivírus (estações de trabalho e servidores), remoto 24x7. Origem: Pessoa jurídica, Fornecimento: 36 meses	UN	

Lote 2

Código do item	ID	Descrição	Unidade de fornecimento	Quantidade estimada
1	167763	Descrição: Subscrição de licenças de uso para solução Antivírus (Dispositivos móveis). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	UN	
2	167765	Serviço de treinamento para solução antivírus (Dispositivos móveis).	Turma	
3	167767	Serviço de suporte técnico para solução antivírus (dispositivos móveis), remoto 24x7. Origem: Pessoa jurídica, Fornecimento: 36 meses	UN	

1.1. Características e Funcionalidades Gerais da Solução Antivírus

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

1.1.2. Analisar arquivos, execuções de memória e tráfego de rede dos endpoints; verificar continuamente os discos rígidos (Hds) e demais mídias de armazenamento de forma transparente ao usuário;

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

1.1.4. Atualizar a lista de ameaças cibernéticas conhecidas, pela rede, de preferência diariamente;

1.1.5. Fornecer visibilidade das ameaças do parque tecnológico do PRODERJ e dos Órgãos do Governo do Estado aderentes a esta Ata;

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

1.1.7. Os itens “1” e “2” do Lote 1, correspondentes a licenças de uso para estações de trabalho e servidores, devem ser gerenciáveis através da console de gerenciamento centralizado;

1.1.8. O conjunto de softwares que compõe a solução de antivírus para estações de trabalho, dispositivos móveis e servidores (físicos e virtualizados) deverão ser compatíveis entre si, de modo a permitir a integração e correlação de eventos de segurança;

1.1.9. Fornecer manuais necessários à instalação, manutenção e utilização da solução, nos seguintes meios: papel, CD e ou Website em Inglês ou Português do Brasil;

1.1.10. Todos os itens do “Lote 1” deverão ser entregues por um único fornecedor, bem como os itens do “Lote 2”. Não será necessário que somente uma empresa ganhe os dois lotes;

1.1.11. 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;

1.1.12. 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);

1.1.13. Possuir console para monitoramento remoto com utilização de interface gráfica (GUI) ou browser para administração, monitoração e gerenciamento da solução ofertada que funcione em plataforma Windows.

2. Funcionalidades Específicas da Solução Antivírus (LOTE 1)

Para comprovação das funcionalidades descritas neste documento, será solicitado catálogo técnico da solução em português ou inglês, e documento constando análise ponto a ponto. Caso se faça necessário para comprovação, poderá ser solicitado ainda teste de bancada.

2.1. Subscrição de licenças de uso para solução Antivírus (estações de trabalho).

2.1.1. A solução deve atender os seguintes sistemas operacionais:

2.1.1.1. Windows 7 (Todas as versões);

2.1.1.2. Windows 8.1 (Standard, Pro e Enterprise);

2.1.1.3. Windows 10 (Todas as versões);

2.1.1.4. OS X 10.12 em diante;

2.1.2. Funcionalidade de Administração e Gerência

2.1.2.1. A console de gerenciamento centralizado deverá estar disponível em nuvem e/ou on-premise;

2.1.2.2. Deve ser possível usar administração de forma hibrida;

2.1.2.3. Em caso de uso on-premise deve ser instalado em Windows 2012 Server ou superior, seja o servidor físico ou virtual;

2.1.2.4. Solução deve suportar base de dados Microsoft SQL Server;

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

2.1.2.6. A console de gerenciamento centralizada deve monitorar e administrar os módulos da solução descritos nos itens abaixo;

2.1.2.7. Deve gerenciar logs das atividades e eventos gerados pela solução;

2.1.2.8. Nas informações da política deve conter informações como nome, status, dono da política, horário e data da última alteração;

2.1.2.9. A gerencia central deverá mostrar quais estações estão sem políticas;

2.1.2.10. Deve gerar relatório de compliance com informações de máquinas que nunca realizaram scan, politicas inconsistentes entre servidor/agente e componentes desatualizados;

2.1.2.11. Deve possuir integração com Microsoft Active Directory;

2.1.2.12. Deve permitir níveis de administração da console por usuários ou grupos de usuários;

2.1.2.13. Deve permitir a constituição de políticas genéricas aplicáveis a máquinas, grupos de usuários ou máquinas;

2.1.2.14. Deve disponibilizar sua interface através dos protocolos http e https;

2.1.2.15. Geração de relatórios e gráficos e parametrizáveis nos formatos html, pdf, xml e csv;

2.1.2.16. Deve gerar relatórios e gráficos pré-definidos nos formatos pdf, docx e xlsx;

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

2.1.2.18. Deve permitir criação de modelos de relatórios customizados;

2.1.2.19. Deve permitir a criação de planos de entrega das atualizações, com hora de início ou postergação da entrega após o download dos componentes;

2.1.2.20. Deve permitir o controle individual de cada componente a ser atualizado;

2.1.2.21. Deve permitir a definição de exceções por dias e horas para não realização de atualizações;

2.1.2.22. Deve permitir ter como fonte de atualização um compartilhamento de rede em pelo menos um dos seguintes formatos: UNC, NFS e SMB;

2.1.2.23. Deve gerar relatórios e gráficos com o detalhamento das versões dos produtos instalados;

2.1.2.24. Deve possuir o acompanhamento dos comandos administrativos em execução, tal como seu status de conclusão, alvo e usuário;

2.1.2.25. Deve permitir a configuração dos eventos administrativos ou de segurança que geram notificações, tal como o método de envio e o destinatário;

2.1.2.26. Os métodos de envio suportados devem incluir ao menos duas das seguintes opções: e-mail, gravação de registros de eventos do Windows, SNMP e SYSlog;

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

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

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

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

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

2.1.2.32. Deve permitir a configuração da duração do bloqueio;

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

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

2.1.2.35. 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;

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

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

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

2.1.2.39. 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;

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

2.1.2.41. 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;

2.1.2.42. 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;

2.1.2.43. Deve possibilitar instalação "silenciosa";

2.1.2.44. Deve permitir o bloqueio por nome de arquivo via prevenção de epidemia;

2.1.2.45. Deve permitir o travamento de pastas e diretórios compartilhados via prevenção de epidemia;

2.1.2.46. Deve permitir o travamento de portas via prevenção de epidemia;

2.1.2.47. Deve permitir o rastreamento e bloqueio de infecções;

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

2.1.2.49. 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;

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

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

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

2.1.2.53. Deve permitir a deleção dos arquivos quarentenados;

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

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

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

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

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

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

2.1.2.60. 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;

2.1.2.61. Deve registrar no sistema de monitoração de eventos da console de antimalware informações relativas ao usuário logado no sistema operacional;

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

2.1.2.63. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;

2.1.2.64. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes;

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

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

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

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

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

2.1.2.70. 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;

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

2.1.2.72. 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;

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

2.1.3. Módulo de Proteção Anti Malware

2.1.3.1. A solução de antimalware deve trabalhar de forma hibrida, fazendo uso de assinaturas, machine learning e detecção de comportamento para identificar malwares no endpoint;

2.1.3.2. A solução deve possuir uma regra pré-definida para análise de malware consultando somente extensões comumente usadas por malware para otimizar o uso de recurso do endpoint;

2.1.3.3. Deve ser possível também definir quais extensões devem ser monitoradas de forma manual ou permitir ler todos os arquivos;

2.1.3.4. Em caso de detecção a solução deve tomar uma das seguintes ações:

- Liberar acesso;
- Quarentenar;
- Limpar;
- Bloquear acesso;
- Deletar;
- Renomar;

2.1.3.5. A solução deve permitir colocar pastas, programas ou arquivos em exclusão para evitar falso positivos e otimizar o uso de recurso;

2.1.3.6. Deve possuir a função SCAN CACHE, otimizando o scan nas máquinas armazenando informações dos arquivos que já são conhecidos como bons otimizando o uso de recurso;

2.1.3.7. Deve ser possível alterar o período que o cache será armazenado para que seja criada uma nova base de assinaturas;

2.1.3.8. Arquivos quarentemados devem ser possíveis de ser restaurados pela console central ou direto no endpoint;

2.1.3.9. Os arquivos quarentenados devem ser criptografados para evitar execução acidental e devem ser acessados com ferramenta provida pelo fornecedor;

2.1.3.10. A solução deve permitir configurar scan baseado em assinaturas ou uso da inteligência na nuvem do fabricante;

2.1.3.11. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, key loggers, programas de propaganda, rootkits, ransomware e fileless;

2.1.3.12. Em caso de cavalos de tróia a solução deve conseguir remover não só o malware mas também todos os processos criados por ele, recuperar alterações feitas em arquivos de sistema e deletar possíveis arquivos baixados pelo trojan;

2.1.3.13. A solução deve permitir scannear o sistema operacional antes do boot em busca de malware “boot-type rootkits”;

2.1.3.14. Para evitar falso positivos com spywares a solução deve permitir um modo de avaliação onde o administrador será notificado, porém as aplicações não são bloqueadas, permitindo criar uma whitelist antes de habilitar o bloqueio;

2.1.3.15. Solução deve permitir conter surtos de malware na rede isolando o endpoint infectado;

2.1.3.16. O administrador deve ser notificado sobre surto na rede através do gerenciador central a partir de políticas definidas pelo administrador;

2.1.3.17. A ação de isolamento do endpoint deve ser executada pelo administrador na console central de gerenciamento;

- Entre as ações tomadas pela contenção de surtos deve ser possível:
- Limitar ou negar acesso a pastas compartilhadas;
- Bloquear portas;
- Negar escrita em arquivos e pastas;
- Negar execução de arquivos executáveis (.exe);

2.1.3.18. Deve ser possível notificar o usuário com uma mensagem customizada;

2.1.3.19. A solução deve possuir um modulo de detecção de comportamento e análise de scripts, bloqueado ameaças conhecidas e potencialmente perigosas;

2.1.3.20. Deve detectar scripts maliciosos mesmo quando executados por aplicações legítimas do Windows;

2.1.3.21. A solução de antivírus deverá possuir funcionalidades especificas para prevenção contra a ação de ransomwares, tais como a capacidade de impedir a criptografia quando feita por aplicativos desconhecidos com a capacidade de fazer backup de arquivos antes de serem criptografados para posteriormente permitir sua restauração.

2.1.3.22 Deve bloquear processos comuns associados a ransomware;

2.1.3.23. Deve proteger contra exploits em arquivos executáveis e arquivos do pacote office;

2.1.3.24. Deve realizar monitoramento da memória em tempo real para detecção de ataques fileless, sendo possível terminar os processos ou quarentenar para análise posterior;

2.1.3.25. Deve realizar monitoramento de eventos no endpoint que possam indicar um comportamento malicioso;

2.1.3.26. Deve permitir monitorar ao menos os seguintes eventos:

- Arquivos de sistema duplicados;
- Modificação no arquivo hosts;
- Novo plugin no Internet Explorer;
- Alteração nas configurações do Internet Explorer;
- Alteração nas políticas de segurança do Windows;
- Injeção na biblioteca de programas;
- Modificação no shell;
- Novo serviço;
- Modificação em arquivo do sistema;
- Alteração na política de firewall;
- Alteração em processos do sistema;
- No programa na inicialização do sistema;

2.1.3.27. Sempre que detectado um evento deve permitir no mínimo as seguintes opções:

- Permitir;
- Bloquear;
- Perguntar quando necessário;
- Avaliar;

2.1.3.28. Deve ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas (zero-day) e suspeitas consultando modelos e características na nuvem do fabricante;

2.1.3.29. O modulo de Machine Learning deverá funcionar em modo off-line caso o agente perca comunicação com a nuvem do fabricante, e deve retomar a conexão com a nuvem do fabricante de forma automática assim que tiver conexão disponível;

2.1.3.30. Modulo de Machine Learning deve usar base do fabricante não sendo necessário que se faça uma base local nos endpoints ou no servidor de gerenciamento

centralizado visando reduzir o número de falso positivos;

2.1.3.31. O modulo de Machine Learning deve monitorar arquivos e processos;

2.1.3.32. O modulo de Machine Learning deve funcionar para análise estática o arquivo e em execução para evitar ofuscação de código malicioso.

2.1.3.33. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

2.1.3.34.. Deve permitir configurar aos menos os seguintes tipos de scanneamento:

- Manual;
- Agendado;
- Tempo-real;

2.1.3.35. Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual e agendada;

2.1.3.36. A solução deve possuir modulo de proteção contra alteração dos arquivos e serviços usados pelo agente de proteção.

2.1.4. Funcionalidade de reputação web

2.1.4.1. A solução deve prover proteção web sem necessidade de instalação de plug-ins nos navegadores;

2.1.4.2. Deve suportar ao menos os seguintes navegadores:

- Google Chrome;
- Mozilla Firefox;
- Microsoft Edge;
- Safari

2.1.4.3. Solução deve detectar site malicioso através da reputação em nuvem do fabricante;

2.1.4.4. Solução deve permitir liberar ou bloquear acesso aos sites de baseado na pontuação atribuída pelo fabricante;

2.1.4.5. O modulo deve bloquear também tentativas de exploits através de sites maliciosos;

2.1.4.6. O modulo deve bloquear uso de scripts ou applets maliciosos através do navegador;

2.1.4.7. A pontuação do fabricante deve conter ao menos 3 níveis:

- Sites perigosos;
- Sites perigoso e altamente suspeitos;
- Sites perigos, altamente suspeitos e suspeitos;

2.1.4.8. Deve ser possível bloquear sites que ainda não foram avaliados pelo fabricante;

2.1.4.9. A solução deve conseguir validar sites que usem protocolo HTTPS;

2.1.4.10. Deve ser possível criar uma whitelist para bypassar a análise do módulo de reputação web para evitar falsos positivos;

2.1.4.11. Deve ser possível habilitar um módulo de avaliação para evitar falsos positivos;

2.1.4.12. A solução deve detectar conexões com IPs conhecidos de C&C e bloquear a conexão em máquinas Windows;

2.1.4.13. Sempre que houve uma detecção de malware no endpoint a solução deve fazer uma checagem para ver se o malware em algum momento se comunicou com uma C&C em máquinas Windows;

2.1.5. Funcionalidade de controle de dispositivos e proteção de dados

2.1.5.1. Deve possuir o controle de acesso a drives de mídias de armazenamento como cdrom, dvd, com as opções de acesso total, leitura e escrita, modificar, listar o conteúdo e bloqueio total;

2.1.5.2. Desejável possuir o controle a drives mapeados com as seguintes opções: acesso total, modificar, leitura e execução, apenas leitura e listar somente o conteúdo;

2.1.5.3. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com uma política aplicada;

2.1.5.4. Possibilidade de adicionar novos dispositivos na lista de dispositivos permitidos utilizando “Class ID”, “Device ID” ou “Serial ID” do dispositivo;

2.1.5.5. A solução deve possuir repositório central de identificadores de dados, que podem ser utilizados para a criação de políticas contra possíveis vazamentos de informações;

2.1.5.6. A proteção contra vazamento de dados deverá verificar o true file type a fim de impedir que o usuário tente burlar a segurança;

2.1.5.7. Deve permitir a criação de modelos personalizados para identificação de informações;

2.1.5.8. Deve permitir mais de uma ação para cada política, como: Apenas registrar o evento da violação, bloquear a transmissão, gerar alerta para o usuário, alertar na central de gerenciamento e solicitar uma justificativa para o usuário;

2.1.5.9. A proteção contra vazamento de dados deve possuir a capacidade de realizar uma busca de arquivos baseado em computadores selecionados baseados em template,

2.1.6. Funcionalidade de Host Firewall e HIPS

2.1.6.1. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host ips e host firewall;

2.1.6.2. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;

2.1.6.3. Todas as regras das funcionalidades de firewall e ips de host devem permitir apenas detecção (log) ou prevenção (bloqueio);

2.1.6.4. Deve permitir ativar e desativar o produto sem a necessidade de remoção;

2.1.6.5. Deve permitir que os administradores habilitem ou desabilitem as regras de IPS;

2.1.6.6. Deverá possuir a possibilidade de configurar níveis diferentes de segurança para o firewall podendo ser eles Alto, médio e baixo;

2.1.6.7. Deverá prevenir contra os seguintes tipos de ataque: Too Big Fragment, Ping da morte, Conflito de ARP, SYN Flood, Overlapping Fragment, Tiny Fragment Attack, Fragmented IGMP e Land Attack;

2.1.6.8. A funcionalidade de HIPS deverá possuir perfis pré-derteminados baseados em performance e segurança;

2.1.6.9. A funcionalidade de HIPS deverá possuir regras para proteger contra ameaças do tipo Ransomware;

2.1.6.10. A funcionalidade de HIPS deverá conter regras contra exploit, vulnerabilidades e genéricas protegendo contra ameaças conhecidas ou desconhecidas;

2.1.7. Módulo para controle de aplicações

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

2.1.7.2. 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;

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

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

2.1.7.5. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: Assinatura sha-1 e sha-256 do executável; Atributos do certificado utilizado para assinatura digital do executável, Caminho lógico do executável, Base de assinaturas de certificados digitais válidos e seguros;

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

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

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

2.1.8. Funcionalidade de criptografia

2.1.8.1. Deve possuir as seguintes funcionalidades de criptografia para as estações de trabalho (desktops e notebooks): Disco completo (fde – full disk encryption);

2.1.8.2. Deve possuir autenticação durante a inicialização (boot) da estação de trabalho, antes do carregamento do sistema operacional, para a funcionalidade de criptografia do disco completo;

2.1.8.3. A autenticação durante a inicialização (boot) deve ser a partir das credenciais sincronizadas com o Active Directory;

2.1.8.4. Deve possuir suporte ao algoritmo de criptografia aes-256;

2.1.8.5. Deve possuir criptografia no canal de comunicação entre as estações de trabalho e o servidor de políticas;

2.1.8.6. Deve possuir funcionalidade de criptografia por software ou hardware;

2.1.8.7. Deve ser compatível com os padrões SED ('self-encrypting drive), opal e opal2

2.1.8.8. Deve possuir compatibilidade de autenticação por múltiplos fatores;

2.1.8.9. Deve permitir atualizações do sistema operacional mesmo quando o disco está criptografado;

2.1.8.10. Deve possuir políticas por usuários, grupos e dispositivos;

2.1.8.11. Deve possuir autoajuda para usuários que esquecerem a senha com a combinação de perguntas e respostas;

2.1.8.12. Deve possuir mecanismos para wipe (limpeza) remoto;

2.1.8.13. Deve possuir mecanismo para desativar temporariamente a autenticação de pré-inicialização (boot);

2.1.8.14. Deve prover ferramenta presente na estação de trabalho que possibilite migrá-la para um servidor de gerenciamento diferente;

2.1.8.15. Deve permitir a visualização do autor de determinada política a partir da console de administração centralizada;

2.1.8.16. Deve permitir a exibição de aviso legal quando o agente de criptografia é instalado na estação de trabalho;

2.1.8.17. Deve possibilitar que cada política tenha uma chave de criptografia única;

2.1.8.18. Deve permitir, em nível de política, a escolha da chave de criptografia a ser utilizada, entre as seguintes opções: Chave do usuário: somente o usuário tem acesso aos arquivos; Chave da empresa: qualquer usuário da empresa tem acesso aos arquivos e Chave da política: qualquer estação de trabalho que tenha aplicada a mesma política tem acesso aos arquivos;

2.1.8.19. Deve possuir integração com o Gerenciamento Centralizado para visibilidade dos dispositivos criptografos e criação de política;

2.2. Subscrição de licenças de uso para solução Antivírus (Servidores)

2.2.1. Deverá ser compatível com no mínimo os sistemas operacionais:

2.2.1.1. Windows:

- Windows Server 2003 R2 SP2 (32/64-bit);
- Windows Server 2008 (32/64-bit);
- Windows Server 2008 R2 (64-bit);
- Windows Server 2012 (64-bit);
- Windows Server 2012 R2 (64-bit);
- Windows Server Core 2012 (64-bit);
- Windows Server Core 2012 R2(64-bit);
- Windows Server 2016 (64-bit);
- Windows Server 2019 1809 (64-bit) e posteriores;

2.2.1.2. Linux:

- Red Hat Enterprise Linux 5 (32-bit);
- Red Hat Enterprise Linux 6 (32/64-bit);
- Red Hat Enterprise Linux 7 (64-bit);
- Red Hat Enterprise Linux 8 (64-bit) e posteriores;
- CentOS 5 (32/64-bit);
- CentOS 6 (32/64-bit);
- CentOS 7 (64-bit);
- CentOS 8 (64-bit) e posteriores;
- Oracle Linux 5 (32/64-bit);
- Oracle Linux 6 (32/64-bit);
- Oracle Linux 7 (64-bit);
- Oracle Linux 8 (64-bit) e posteriores;
- SUSE Linux Enterprise Server 11 (32/64-bit);
- SUSE Linux Enterprise Server 12 (64-bit) e posteriores;
- Ubuntu 10.04 LTS (64-bit);
- Ubuntu 14 (64-bit);
- Ubuntu 16 (64-bit);
- Ubuntu 18.04 (64-bit);
- Ubuntu 20.04 (64-bits) e posteriores;
- Debian 7 (64-bit);
- Debian 8 (64-bit);
- Debian 9 (64-bit);
- Debian 10 (64-bit) e posteriores;

2.2.2. Deverá ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes:

- Hyper-V
- Vmware
- Red Hat Virtualization - RHV

2.2.3. 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;

2.2.4. Deverá permitir no mínimo a aplicação de regras de IPS/IDS e antimalware para hosts gerenciados de Docker container;

2.2.5. 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;

2.2.6. Desejável ter a capacidade de se integrar com os principais softwares de SIEMs de mercado, no mínimo com: Ossim, IBMQradar, Splunk e ArcSight, de modo a permitir enviar os seus logs para essas soluções;

2.2.7. Deverá possibilitar enviar logs para SYSLOG servers;

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

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

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

2.2.10.1. Executar tarefas de manutenção de rotina;

2.2.10.2. Configurar políticas e proteger servidores;

2.2.10.3. Pesquisar políticas por nome

2.2.11. Configurações de proteção antimalware:

2.2.11.1. Definir as configurações da varredura antimalware em tempo real;

2.2.11.2. Configurar exclusões de diretório para uma configuração de varredura de malware;

2.2.11.3. Obter as configurações antimalware de todos os servidores;

2.2.11.4. Gerar relatório referente ao status do módulo;

2.2.12. Configurações de proteção contra URLs maliciosas:

2.2.12.1. Ativar a proteção contra URLs maliciosas;

2.2.12.2. Definir configurações;

2.2.12.3. Gerar relatório referente ao status do módulo;

2.2.13. Configurações de controle de firewall de host:

2.2.13.1. Configurar firewall;

2.2.13.2. Realizar pesquisa de regra de firewall por nome;

2.2.13.3. Gerar relatório referente ao status do módulo;

2.2.14. Configurações de proteção contra exploração de vulnerabilidades:

2.2.14.1. Definir configurações de prevenção de intrusões;

2.2.14.2. Realizar busca para identificar regra de prevenção de intrusões para uma CVE;

2.2.14.3. Realizar busca para identificar regra servidores que não estão protegidos contra uma CVE;

2.2.14.4. Descobrir e aplicar automaticamente regras IDS/IPS que blindem exploração das vulnerabilidades existentes no sistema operacional e aplicações;

2.2.14.5. Gerar relatório referente ao status do módulo;

2.2.15. Configurações do monitoramento de integridade e rastreabilidade:

2.2.15.1. Adicionar regras de monitoramento de integridade e rastreabilidade a uma política;

2.2.15.2. Gerar relatório referente ao status do módulo;

2.2.16. Configurações da inspeção de log:

2.2.16.1. Adicionar regra de inspeção de log a uma política;

2.2.16.2. Criar uma regra de inspeção de log;

2.2.16.3. Gerar relatório referente ao status do módulo;

2.2.17. Configurações de controle de aplicação:

2.2.17.1. Ativar controle de aplicações;

2.2.17.2. Bloquear softwares não reconhecidos;

2.2.17.3. Ativar o modo de manutenção;

2.2.17.4. Gerar relatório referente ao status do módulo;

2.2.17.5. Gerar relatório sobre o status do agente;

2.2.17.6. Gerar script de instalação do agente;

2.2.17.7. Autenticação – Log in e Log out;

2.2.17.8. Administração de Contas - Criação, edição e exclusão de contas de acesso;

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

2.2.18. 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.

2.2.2. Proteção antimalware

2.2.2.1. Deverá possuir proteção antimalware baseada em agente;

2.2.2.2. Deverá possuir proteção antimalware com serviço de reputação externa através de nuvem de inteligência do próprio fabricante;

2.2.2.3. Deverá possuir validação reputacional estendida com prevalência e contador de execuções;

2.2.2.4. Deverá possuir proteção antimalware convencional com padrões locais;

2.2.2.5. Deverá suportar proteção antimalware sem agente baseado em Vmware API (NSX-V);

2.2.2.6. Deverá possibilitar realizar a varredura de arquivos sem utilização de agente, evitando a varredura de conteúdos duplicados (VMware Scan Cache);

2.2.2.7. Deverá possibilitar configurar cache de varredura e exclusões para varreduras sem agente;

2.2.2.8. Deverá ser compatível com no mínimo os seguintes sistemas operacionais: Windows Server 2008 (32/64-bit), Windows Server 2008 R2 (64-bit), Windows Server 2012 (64-bit); Windows Server 2012 R2 (64-bit); Windows Server 2016 (64-bit) e Windows Server 2019.

2.2.2.9. A solução deve possuir um cache dos arquivos verificados de modo a evitar a redundância da varredura;

2.2.2.10. O cache de arquivos verificados deverá estar disponível para varredura sob demanda e varredura em tempo real;

2.2.2.11. Deverá possibilitar ao administrador liberar os arquivos quarentenados tanto no modo sem agente quanto no modo com agente;

2.2.2.12. Deverá possuir proteção em tempo real;

2.2.2.13. Deverá possibilitar diferentes configurações de detecção (varredura ou rastreamento):

- Manual;
- Agendado;

2.2.2.14. Deverá possibilitar configurar o modo de I/ O para proteção em tempo real:

- Escrita / leitura;
- Somente escrita;
- Somente leitura;

2.2.2.15. Deverá possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar impactos de performance no host;

2.2.2.16. Deverá possuir análise de comportamento visando identificar ameaças desconhecidas;

2.2.2.17. Deverá possuir proteção contra ransomware utilizando de gatilhos do sistema em tentativas de criptografia;

2.2.2.18. Deverá realizar backup dos arquivos afetados por tentativas de criptografia, possibilitando a restauração assim que o sistema for limpo;

2.2.2.19. A solução deve ter capacidade de monitorar processos legítimos contra realizações de ações que não são tipicamente realizadas pelos mesmos, a fim de detectar e bloquear ameaças;

2.2.2.20. Deverá realizar varredura de arquivos de pré-execução utilizando machine learning;

2.2.2.21. Deverá identificar CVE de dia zero em documentos office e PDF;

2.2.2.22. Deverá possuir proteção contra spyware;

2.2.2.23. Deverá realizar varredura de arquivos comprimidos;

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

2.2.2.25. Deverá ser possível configurar no mínimo 5 (cinco) camadas;

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

2.2.2.27. Deverá realizar a varredura de pastas de rede;

2.2.2.28. A solução deverá possibilitar a criação de listas de inclusão para que o processo do antivírus execute a varredura de determinados diretórios e arquivos;

2.2.2.29. A solução deverá possibilitar a criação de listas de exclusão para que o processo do antivírus não execute a varredura de determinados diretórios e arquivos;

2.2.2.30. Deverá permitir configurar o consumo de CPU que será utilizado para varredura manual e/ou agendada;

2.2.2.31. Deverá suportar processamento multitarefa;

2.2.3. Proteção contra URL`s maliciosas

2.2.3.1. Deverá possuir proteção baseada em agente contra acesso a URLs maliciosas utilizando classificação de reputação;

2.2.3.2. Deverá suportar proteção contra URLs maliciosas antimalware sem agente baseado em Vmware API(NSX-V);

2.2.3.3. Deverá possuir limiares configuráveis para bloquear o controle de sensibilidade;

2.2.3.4. Deverá possuir porta configuráveis para controle de atividade da web;

2.2.3.5. Deverá possibilitar criar blacklist e whitelist de URLs:

2.2.3.5.1. Domínio;

2.2.3.5.2. URL;

2.2.3.5.3. Palavras chaves;

2.2.3.6. Deverá possuir serviços de reputação configuráveis para lidar com solicitações (global ou local);

2.2.3.7. O serviço de reputação e a base de reputação devem ser do mesmo fabricante que provê a solução deproteção de servidores;

2.2.3.8. Deverá possibilitar configurar a engine:

- Inline;

- Tap – possibilitando realizar testes;

2.2.4. Firewall de host

2.2.4.1. Deverá trabalhar como firewall de host, através da instalação de agente nos servidores protegidos;

2.2.4.2. Deverá ter a capacidade de controlar o tráfego baseado no endereço MAC, frame types, tipos de protocolos, endereços IP e intervalo de portas;

2.2.4.3. Deverá ter a capacidade de definir regras distintas para interfaces de rede distintas;

2.2.4.4. Deverá ter a capacidade de controlar conexões TCP baseado nas Flags TCP;

2.2.4.5. Deverá ser capaz de reconhecer e possibilitar o bloqueio de endereços IP que estejam realizando network Scan, Port Scan, TCP Null Scan, TCP FYNSYN Scan, TCP Xmas Scan e Computer OS Fingerprint;

2.2.4.6. Deverá ter a capacidade de implementação de regras em determinados horários, customizados pelo administrador;

2.2.4.7. Deverá ter a capacidade de definição de regras para contextos específicos;

2.2.4.8. Deverá ter a capacidade de realização de varredura de portas nos servidores;

2.2.4.9. As 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);

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

2.2.4.11. Para facilitar a criação e administração de regras de firewall, as mesmas poderão ser baseadas em objetos que podem ser lista de IPs e lista de portas;

2.2.4.12. Deverá ser stateful bidirecional;

2.2.4.13. Deverá permitir liberar ou apenas logar eventos;

2.2.4.14. Deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

2.2.4.15. Deverá possuir as seguintes ações, ou equivalentes: permitir, apenas logar, bloquear, bypass e forçar permissão;

2.2.4.16. Deverá utilizar o conceito de regras implícitas para as regras de permissão, negando o tráfego para todo o restante que não estiver liberado;

2.2.4.17. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

2.2.4.18. Deverá realizar pseudo stateful em tráfego UDP;

2.2.4.19. Deverá logar a atividade stateful;

2.2.4.20. Deverá permitir limitar o número de conexões de entrada e o número de conexões de saída de um determinado servidor;

2.2.4.21. Deverá prevenir ack storm;

2.2.4.22. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

2.2.4.23. Poderá atuar no modo inline para proteção contra ataques ou modo escuta para monitoração e alertas;

2.2.5. Proteção contra exploração de vulnerabilidades

2.2.5.1. Deverá possuir proteção contra exploração de vulnerabilidades baseada em agente;

2.2.5.2. Desejável suportar proteção contra exploração de vulnerabilidades e sem agente baseado em Vmware API (NSX-V); não sendo nesse caso, necessário inspecionar tráfego de entrada SSL;

2.2.5.3. Deverá detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do sistema operacional e aplicações;

2.2.5.4. Deverá realizar auditoria automática do servidor protegido (agendada e manual), detectando o tipo e versão do sistema operacional, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem exploração das vulnerabilidades existentes no sistema operacional e aplicações.

2.2.5.5. Deverá definir e desabilitar automaticamente as regras relevantes com base na auditoria realizada para adaptar o perfil de segurança (no caso de a vulnerabilidade já ter sido solucionada, a regra deverá ser removida automaticamente; e vice-versa).As regras deverão ser ativadas para as vulnerabilidades recém-descobertas e sistema sendo protegido por patch virtual.

2.2.5.6. Deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

2.2.5.7. Deverá detectar conexões maliciosas, com a possibilidade de bloquear esta conexão.

2.2.5.8. A opção de detecção e bloqueio deverá possibilitar ser implementada de forma global (todas as regras) e apenas para uma regra ou grupos de regras;

2.2.5.9. Deverá possuir regras de defesa para blindagem de vulnerabilidades e ataques que explorem os sistemas operacionais supracitados e regras para aplicações/serviços padrões de mercado, incluindo Microsoft IIS, DNS, SQL Server, Microsoft Exchange, Oracle Database,PostgreSQL, Adobe Acrobat, Tomcat,Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Red Hat Jboss, JAVA, PHP, Wordpress, Weblogic, soluções de backup, bibliotecas linux, Citrix, e Web Server Apache;

2.2.5.10. Deverá realizar o armazenamento do pacote capturado quando detectado um ataque;

2.2.5.11. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações próprias;

2.2.5.12. Deverá detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e mensagens instantâneas;

2.2.5.13. Deverá detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting.

2.2.5.14. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: Sql injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

2.2.5.15. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

2.2.5.16. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de

sistemas web legados e/ou proprietários;

2.2.5.17. Deverá possibilitar permitir ou bloquear métodos utilizados por Webservers por regras de IPS;

2.2.5.18. As 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);

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

2.2.5.20. Deverá ser capaz de inspecionar tráfego de entrada SSL;

2.2.5.21. Deverá apresentar informações detalhadas das regras de proteção contra vulnerabilidades, contendo links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante e CVE relacionado;

2.2.5.22. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

2.2.5.23. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

2.2.5.24. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

2.2.5.25. Deverá possibilitar habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para realizar análise;

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

2.2.5.27. Deverá ser possível configurar o modo de detecção, possibilitando apenas detectar ou bloquear os eventos que violem as regras, de modo que o administrador possa optar por qual ação tomar;

- As regras de proteção de vulnerabilidade deverão:
- Apresentar severidade baseada em CVE's;
- Apresentar CVE relacionado a vulnerabilidade e/ou a regra de IPS;
- Ter capacidade de LOG desabilitado;
- Quando disparadas poderão ter a possibilidade de emitir um alerta;
- Ser atualizadas automaticamente pelo fabricante;

2.2.5.28. Deverá ser possível configurar o modo de detecção, possibilitando atuar no modo em linha para proteção contra ataques e modo escuta para monitoração e alertas;

2.2.6. Monitoramento de integridade e rastreabilidade

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

2.2.6.2. Desejável suportar monitoramento de integridade e rastreabilidade sem agente baseado em Vmware API (NSX-V);

2.2.6.3. Desejável que a solução permita o monitoramento de integridade de arquivos na máquina virtual (VMWARE) a ser monitorada;

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

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

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

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

2.2.6.8. Deverá monitorar mudanças efetuadas no registro do Windows;

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

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

2.2.6.11. 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;

2.2.6.12. 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);

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

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

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

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

2.2.6.17. 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;

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

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

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

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

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

2.2.7. Inspeção de Logs

2.2.7.1. 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;

2.2.7.2. 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;

2.2.7.3. 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);

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

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

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

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

2.2.7.8. Deverá suportar sintaxe OSSEC padrão aberto;

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

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

2.2.8. Controle de Aplicações

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

2.2.8.2. Deverá possuir as seguintes configurações ou semelhante:

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

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

2.2.8.3. 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;

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

2.2.8.5. 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.

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

2.2.8.7. Deve também realizar o controle de aplicativos em:

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

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

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

2.2.8.7.4. Scripts do Windows PowerShell, batch (.bat) e outros scripts específicos do Windows (.wsf, .vbs, .js)

2.2.8.8. 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".

2.2.9. Funcionalidades de Gerenciamento

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

2.2.9.2. O gerenciamento da console web deverá suportar no mínimo os navegadores Firefox, Internet Explorer, Microsoft Edge, Google Chrome e Apple Safari;

2.2.9.3. Em ambiente on-premises, a console de gerenciamento deverá ser compatível de instalação no mínimo nos seguintes sistemas operacionais:

- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016
- Windows 2019
- RHEL 5
- RHEL 6
- RHEL 7
- RHEL 8

2.2.9.4. 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);

2.2.9.5. Deverá permitir o envio de notificações via SMTP;

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

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

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

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

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

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

2.2.9.12. Deverá permitir que a distribuição de atualizações e novos componentes possa ser efetuada por replicadores espalhados pelo ambiente;

2.2.9.13. A console de gerenciamento deverá permitir alta disponibilidade em nível de aplicação, através da criação de várias consoles, de modo que na ausência da principal, os agentes automaticamente se comuniquem com a secundária e com todas as configurações preservadas;

2.2.9.14. Quando operadas em modo alta disponibilidade, as consoles devem compartilhar o mesmo banco de dados;

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

2.2.9.16. 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;

2.2.9.17. A console deverá permitir que os usuários recebam determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

2.2.9.18. Quando o acesso for configurado em modo parcial, este deve permitir que um usuário possa gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível editar ou criar novas políticas de segurança;

2.2.9.19. Deverá permitir a criação de relatórios, sob demanda, ou agendados, com o envio automático via e-mail, no formato PDF;

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

- PostgreSQL
- Microsoft SQL Server
- Oracle database;

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

2.2.9.22. 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;

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

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

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

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

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

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

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

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

2.2.9.31. 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:

- Hostname;
- Sistema Operacional;
- Docker Host;
- Política de Configurações;
- Active Directory Name/Folder.

2.3. Serviço de treinamento para solução Antivírus

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

2.3.2. 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;

2.3.3. O evento abordará no mínimo: o uso da ferramenta, instalação, configuração, administração, backup e restauração de configuração, gerenciamento, resolução de problemas, utilização da solução e poderá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE;

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

2.3.5. 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;

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

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

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

2.3.9. A carga horária será de até 40 (quarenta) horas para até 1 turma de até 8 (oito) alunos;

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

2.3.11 Os horários e datas dos treinamentos serão definidos pela equipe técnica da Contratante e comunicados a Contratada com antecedência de 10 (dez) dias;

2.3.12. 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;

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

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

2.4. Serviço de suporte técnico para solução Antivírus - remoto 24x7

2.4.1. O suporte técnico será remoto, com período de disponibilidade de 24 horas por dia, 7 dias por semana;

2.4.2. Em caso de interrupção ou indisponibilidade do serviço, a contratada se compromete a realizar as correções necessárias à reativação do serviço e a prevenção de novas interrupções, respeitando os prazos de atendimento;

2.4.3. Entende-se por “indisponibilidade total” quando os serviços não estão acessíveis, e “indisponibilidade parcial” quando há degradação dos serviços;

2.4.4. A abertura de chamados de suporte deve possibilitar, no mínimo, os seguintes métodos: via telefone, e-mail, website do fornecedor;

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

2.4.6. Os serviços de suporte técnico deverão contemplar as manutenções corretivas e evolutivas para a solução contratada e não poderão acarretar custos adicionais ao CONTRATANTE, além do contratado, salvo se o problema não estiver relacionado ao objeto do contrato;

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

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

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

2.4.10. A CONTRATADA deverá manter registro de todo o serviço de manutenção e garantia executado, que poderá ser solicitado a qualquer tempo pela contratante;

2.4.11. A contratante poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência do contrato. A contratada deverá possuir contrato de suporte técnico com o fabricante do produto oferecido, a fim de garantir o serviço prestado;

2.4.12. Todos os chamados abertos, por qualquer meio, deverão ser registrados via sistema, e ao final de cada mês será emitido um relatório gerencial e um relatório técnico com todas as informações sobre os atendimentos realizados;

2.4.13. A contratada deverá manter histórico de cada atendimento de suporte realizado, contendo a identificação do problema, providências adotadas e demais informações pertinentes;

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

3. Funcionalidades Específicas da Solução Antivírus (LOTE 2)

3.1. Subscrição de licenças de uso para solução Antivírus (Dispositivos móveis)

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

3.1.1.1. Android 8.0 em diante;

3.1.1.2. iOS 10 em diante;

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

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

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

3.1.5. Deve possuir capacidade de detecção de spam proveniente de SMS;

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

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

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

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

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

3.1.11. 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;

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

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

3.1.14. Deve realizar scan de vulnerabilidades no smartphone;

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

3.1.16. Deve permitir o bloqueio de aplicativos;

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

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

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

3.1.20. Deve possuir integração com o Gerenciamento Centralizado para visibilidade dos dispositivos moveis, single sign on e recebimento de políticas.

3.2. Serviço de treinamento para solução Antivírus (dispositivos móveis)

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

3.2.2. 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;

3.2.3. O evento abordará no mínimo: o uso da ferramenta, instalação, configuração, administração, backup e restauração de configuração, gerenciamento, resolução de problemas, utilização da solução e poderá ser gravado para fins de documentação, caso seja de interesse da CONTRATANTE;

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

3.2.5. 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;

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

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

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

3.2.9. A carga horária será de até 40 (quarenta) horas para até 1 turma de até 8 (oito) alunos;

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

3.2.11. Os horários e datas dos treinamentos serão definidos pela equipe técnica da Contratante e comunicados a Contratada com antecedência de 10 (dez) dias;

3.2.12. 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;

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

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

3.3. Serviço de suporte técnico para solução Antivírus (dispositivos móveis) - remoto 24x7

3.3.1. O suporte técnico será remoto, com período de disponibilidade de 24 horas por dia, 7 dias por semana;

3.3.2. Em caso de interrupção ou indisponibilidade do serviço, a contratada se compromete a realizar as correções necessárias à reativação do serviço e a prevenção de novas interrupções, respeitando os prazos de atendimento;

3.3.3. Entende-se por “indisponibilidade total” quando os serviços não estão acessíveis, e “indisponibilidade parcial” quando há degradação dos serviços;

3.3.4. A abertura de chamados de suporte deve possibilitar, no mínimo, os seguintes métodos: via telefone, e-mail, website do fornecedor;

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

3.3.6. Os serviços de suporte técnico deverão contemplar as manutenções corretivas e evolutivas para a solução contratada e não poderão acarretar custos adicionais ao CONTRATANTE, além do contratado, salvo se o problema não estiver relacionado ao objeto do contrato;

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

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

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

3.3.10. A CONTRATADA deverá manter registro de todo o serviço de manutenção e garantia executado, que poderá ser solicitado a qualquer tempo pela contratante;

3.3.11. A contratante poderá efetuar um número ilimitado de chamados de suporte técnico durante a vigência do contrato. A contratada deverá possuir contrato de suporte técnico com o fabricante do produto oferecido, a fim de garantir o serviço prestado;

3.3.12. Todos os chamados abertos, por qualquer meio, deverão ser registrados via sistema, e ao final de cada mês será emitido um relatório gerencial e um relatório técnico com todas as informações sobre os atendimentos realizados;

3.3.13. A contratada deverá manter histórico de cada atendimento de suporte realizado, contendo a identificação do problema, providências adotadas e demais informações pertinentes;

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

4. Demais requisitos da solução antivírus

4.1. Instalação e Configuração

4.1.1. 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;

4.1.2. Após a reunião de kick-off deve ser produzida uma ata, assinada por todos os participantes da CONTRATADA e da CONTRATANTE presentes, 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;

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

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

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

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

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

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

4.1.9. 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;

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

4.1.10.1. Caberá a CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação dos PRODUTOS;

4.1.10.2. 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.

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

4.2. Garantia do Fabricante

4.2.1. A garantia do fabricante dos produtos fornecidos deve obrigatoriamente prover:

4.2.1.1. Atualização dos softwares fornecidos, se novas versões forem disponibilizadas;

4.2.1.2. Atualização dos softwares fornecidos se houver lançamento de novos softwares em substituição aos fornecidos, o mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos;

4.2.1.3. As atualizações acima referidas devem ser implementadas mediante aprovação da contratante;

4.2.1.4. A contratada deverá garantir o funcionamento das consoles de gerenciamento mesmo que haja incompatibilidade com outros softwares da contratante;

4.2.2. Todos os serviços contratados deverão possuir garantia do fabricante durante o período de 36 (trinta e seis) meses a partir da assinatura do Termo de Recebimento Definitivo, incluindo atualização irrestrita do software para a última versão existente, sem qualquer ônus adicional à CONTRATANTE;

4.2.3. Durante todo o período de garantia, o suporte técnico será prestado pela Contratada, que deverá ser devidamente credenciada pelo fabricante para esta finalidade;

4.2.4. A garantia deverá cobrir todo e qualquer defeito apresentado pelo software, incluindo ajustes, reparos e demais correções necessárias;

4.2.5. O fornecedor deverá emitir certificado de garantia junto ao fabricante de 36 (trinta e seis) meses para as licenças entregues;

4.2.6. Em caso de descontinuidade dos componentes da solução de segurança ofertada, a contratada deverá fornecer a nova linha de produto, devidamente homologada, sem quaisquer ônus para a Contratante.

Rio de Janeiro, 09 setembro de 2021

Documento assinado eletronicamente por **Marcelo Soares Lintomen**, **Diretor**, em 10/09/2021, às 23:03, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 10/09/2021, às 23:07, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **21956046** e o código CRC **932B27A4**.

Referência: Processo nº SEI-120211/000548/2020	SEI nº 21956046

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

Criado por prmrei, versão 7 por prmrei em 09/09/2021 20:26:59.

ANEXO II DO TERMO DE REFERÊNCIA
MODELO DE TERMO DE RECEBIMENTO DEFINITIVO

Este presente termo visa atestar que os produtos e serviços prestados pela empresa [NOME DA EMPRESA] por ocasião do Contrato n° / , foram fornecidos e homologados pelos fiscais do contrato em conjunto com o gestor do contrato.

O [ÓRGÃO] recebeu e homologou os seguintes produtos e serviços:

ITEM	DESCRIÇÃO	QUANTIDADE

Informa-se que todos os requisitos do Edital referente a esta contratação foram cumpridos e que a aceitação do objeto está ratificada.

Encaminha-se à empresa CONTRATADA.

[CIDADE],_____de_____de_____.

Fiscal Técnico	Fiscal Requisitante	Gestor do Contrato

(*) Trata-se de um modelo de referência, podendo ser aperfeiçoado durante a execução contratual.

Rio de Janeiro, 09 setembro de 2021

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 10/09/2021, às 23:07, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **21956632** e o código CRC **C273A9E5**.

Referência: Processo nº SEI-120211/000548/2020	SEI nº 21956632

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

Criado por prmrei, versão 5 por prmrei em 09/09/2021 20:13:59.

ANEXO III DO TERMO DE REFERÊNCIA
DECLARAÇÃO DE NÃO UTILIZAÇÃO DE PRODUTOS PERIGOSOS E ADERÊNCIA AOS REQUISITOS DE SUSTENTABILIDADE AMBIENTAL

Atestamos, para fins de comprovação junto à COMISSÃO DE LICITAÇÃO – [ÓRGÃO], relativamente ao Edital n°____/____, que a empresa [NOME DA EMPRESA], CNPJ_____, não emprega substâncias perigosas em seu processo de produção, de acordo com as exigências do Edital.

[CIDADE],_____de_____de_____.

Representante do Fornecedor:

Nome (*):_____

RG:_____CPF: _____

_____

Representante da Empresa / Carimbo

(*) Apresentar ato constitutivo que subscreva a pessoa a representar o fabricante.

Rio de Janeiro, 09 setembro de 2021

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 10/09/2021, às 23:07, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **21956876** e o código CRC **AF348275**.

Referência: Processo nº SEI-120211/000548/2020	SEI nº 21956876

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

Criado por prmrei, versão 2 por prmrei em 09/09/2021 15:59:29.

ANEXO IV DO TERMO DE REFERÊNCIA
MODELO DA ORDEM DE SERVIÇO

1. IDENTIFICAÇÃO DA ORDEM DE SERVIÇO

N°da OS [XXX/XXXX]	Data de Emissao [XX/XX/XXXX]	N° do Contrato [XXX/XXXX]	Data do Contrato [XX/XX/XXXX]

2. IDENTIFICAÇÃO DA EMPRESA CONTRATADA

Nome da Empresa:		
CNPJ:	Inscrição Estadual:	
Endereço:		
Cidade:	UF:	
CEP:	Telefone:	E-mail:

3. PRODUTOS / SERVIÇOS A SEREM FORNECIDOS

Descrição					
Localidade/Endereço	Item	Quantidade	Data (*)	Valor	Servidor Responsável pelo Recebimento
Valor Total					

(*)Observar prazos máximos do Edital

4. APLICAÇÃO DE MULTAS E GLOSAS

A análise da execução dos serviços permite concluir pelo encerramento da Ordem de Fornecimento, com as seguintes observações:

RELATÓRIO DE GLOSAS

[ANEXAR O TERMO DE RECEBIMENTO DEFINITIVO E PARECER DOS FISCAIS]

[CIDADE],____de_____de_____.

_____	_____
Gestor / Carimbo	Empresa / Carimbo

5. ENCERRAMENTO DA ORDEM DE FORNECIMENTO

A análise da execução dos serviços permite concluir pelo encerramento da Ordem de Fornecimento, com as seguintes observações:

[CIDADE],____de_____de_____.

_____

Gestor / Carimbo

(*) Trata-se de um modelo de referência, podendo ser aperfeiçoado durante a execução contratual.

Rio de Janeiro, 09 setembro de 2021

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 10/09/2021, às 23:08, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

A autenticidade deste documento pode ser conferida no site http://sei.fazenda.rj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=6, informando o código verificador **21957255** e o código CRC **8D3E8475**.

Referência: Processo nº SEI-120211/000548/2020	SEI nº 21957255

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

Criado por prmrei, versão 5 por prmrei em 09/09/2021 16:01:58.

ANEXO V DO TERMO DE REFERÊNCIA
MODELO DE PLANILHA DE CUSTOS

Processo SEI Nº_____

Ata de Registro de Preços Nº____/____

Fornecedor:

OBJETO: Registro de Preços para 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, conforme especificações e condições constantes neste Termo de Referência e seus anexos.

LOTE	ID SIGA	Descrição	Unidade de Fornecimento	Quantidade	Valor Unitário	Valor Total
1	167761	Descrição: Subscrição de licenças de uso para solução Antivírus (Estações de trabalho). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	Unidade			
	167762	Descrição: Subscrição de licenças de uso para solução Antivírus (Servidores). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	Unidade			
	167764	Serviço de treinamento para solução antivírus (Estações de trabalho e Servidores)	Turma			
	167766	Serviço de suporte técnico para solução antivírus (estações de trabalho e servidores), remoto 24x7. Origem: Pessoa jurídica, Fornecimento: 36 meses	Unidade			
2	167763	Descrição: Subscrição de licenças de uso para solução Antivírus (Dispositivos móveis). Origem: Pessoa jurídica, Forma Fornecimento: 36 meses	Unidade			
	167765	Serviço de treinamento para solução antivírus (Dispositivos móveis).	Turma			
	167767	Serviço de suporte técnico para solução antivírus (dispositivos móveis), remoto 24x7. Origem: Pessoa jurídica, Fornecimento: 36 meses	Unidade			
Valor Total a pagamento Lote 01:						
Valor Total a pagamento Lote 02:						
Valor Total a pagamento:						

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

Rio de Janeiro, 09 setembro de 2021

Documento assinado eletronicamente por **Manuelito de Sousa Reis Junior**, **Gerente**, em 10/09/2021, às 23:08, conforme horário oficial de Brasília, com fundamento nos art. 21º e 22º do Decreto nº 46.730, de 9 de agosto de 2019.

Referência: Processo nº SEI-120211/000548/2020	SEI nº 21956931

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

Criado por prmrei, versão 2 por prmrei em 09/09/2021 15:54:04.