



CO-05.06/2021

PROCESSO SEI Nº 7010.2021/0004904-7

MODALIDADE DE CONTRATAÇÃO: PREGÃO ELETRÔNICO Nº 05.002/2021

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM FORNECIMENTO DE ATUALIZAÇÕES DE LICENÇAS DE USO PARA 37.000 LICENÇAS DA SUÍTE ANTIVÍRUS MCAFEE MV2 – MVISION PROTECT PLUS, CONTENDO ANTIVÍRUS ENS (ENDPOINT SECURITY), FIREWALL FOR ENDPOINT, WEB CONTROL, DEVICE CONTROL, ATP (ADAPTIVE THREAT PROTECTION), TIE (THREAT INTELLIGENCE EXCHANGE), APPLICATION CONTROL, EPO ON PREMISES, 800 LICENÇAS DE MFE MOVE AV FOR VIRTUAL SERVERS, 1 LICENÇA MFE VIRUSSCAN FOR STORAGE PARA NAS, FORNECIMENTO DE NOVAS LICENÇAS PARA 37.800 ATD (ADVANCED THREAT DEFENSE APPLICANCE), 3 LICENÇAS MFE VIRUSSCAN FOR STORAGE PARA NAS, FORNECIMENTO DE 5 SERVIDORES PARA APLICAÇÃO E BANCO DE DADOS, SUPORTE ESPECIALIZADO ENHANCED SUCCESS PLAN E SERVIÇO DE SUPORTE E MANUTENÇÃO PARA TODA A SOLUÇÃO, PELO PRAZO DE 36 MESES.

CONTRATANTE: EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO – PRODAM-SP S/A, com sede na Rua Líbero Badaró n.º 425, bairro Centro, no Município de São Paulo, no Estado de São Paulo, CEP 01.009-000, inscrita no CNPJ sob n.º 43.076.702/0001-61, neste ato representada por seu Diretor de Administração e Finanças, Sr. **JORGE PEREIRA LEITE** e por seu Diretor de Infraestrutura e Tecnologia, Sr. **ALEXANDRE GEDANKEN**.

CONTRATADA: ISH TECNOLOGIA S/A, com sede na Rua Judith Maria Tovar Varejão n.º 355 – salas 202/203 – Condomínio Edifício Sede ISH, bairro Enseada do Sua, no Município de Vitória, no Estado do Espírito Santo, CEP 29.050-360, inscrita no CNPJ sob n.º 01.707.536/0001-04, neste ato representada por seu Procurador, Sr. **RENATO TENÓRIO**, portador da Cédula de Identidade RG n.º 19.953.787-SSP/SP e inscrito no CPF/MF sob o n.º 176.164.698-25.

As partes acima qualificadas resolveram, de comum acordo, celebrar o presente contrato, mediante as seguintes cláusulas e condições:

CLÁUSULA I – OBJETO

- 1.1. O presente contrato tem por objeto a **Contratação de empresa especializada em fornecimento de atualizações de licenças de uso para 37.000 licenças da Suite Antivírus McAfee MV2 – Mvision Protect Plus contendo Antivírus ENS (Endpoint Security), Firewall for Endpoint, Web Control, Device Control, ATP (Adaptive Threat Protection), TIE (Threat Intelligence Exchange), Application**

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 4525 - Centro - CEP: 01009-000 - São Paulo - SP
prodam.sp.gov.br | prodam@prodam.sp.gov.br



CO-05.06/2021

Control, ePO On Premises, 800 licenças de MFE Move AV For Virtual Servers, 1 licença MFE VirusScan for Storage para NAS, fornecimento de novas licenças para 37.800 ATD (Advanced Threat Defense Appliance), 3 licenças MFE VirusCan for Storage para NAS, fornecimento de 5 servidores para aplicação e banco de dados, Suporte Especializado Enhanced Success Plan e Serviço de Suporte e Manutenção para toda a solução, pelo prazo de 36 meses, conforme descrições constantes no Termo de Referência – Anexo I, da Proposta Comercial da CONTRATADA (doc. SEI 045620347) e demais documentos constantes do processo administrativo em epígrafe.

CLÁUSULA II – OBRIGAÇÕES DA CONTRATADA E CONTRATANTE

2.1. São obrigações da CONTRATADA:

- a) Cumprir fielmente todas as obrigações estabelecidas no Termo de Referência – Anexo I deste instrumento, mormente com as obrigações contidas no item 9 do referido documento, garantindo a qualidade dos serviços prestados;
- b) Para a assinatura do Instrumento Contratual, a CONTRATADA deverá apresentar todos os documentos relativos à regularidade fiscal, e ainda estar em situação regular junto ao CADIN (Cadastro Informativo Municipal) do **Município de São Paulo (Lei Municipal n.º 14.094/2005 e Decreto Municipal n.º 47.096/2006)**, mediante consulta ao site <http://www3.prefeitura.sp.gov.br/cadin/>.
- c) Manter durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de qualificação exigidas no momento da contratação, podendo a CONTRATANTE exigir, a qualquer tempo durante a vigência do contrato, a comprovação das condições que ensejaram sua contratação, devidamente atualizadas e o envio mensal das certidões a seguir elencadas, em formato digital (arquivo PDF) para o e-mail contratosfornecedores@prodam.sp.gov.br e para o gestor do contrato a ser definido oportunamente:
 - i. Certidão Negativa de Débitos relativa aos Tributos Federais e a Dívida Ativa;
 - ii. Certidão de Regularidade do FGTS (CRF);
 - iii. Certidão Negativa de Débitos Tributários e da Dívida Ativa Estadual;
 - iv. Certidão Negativa de Débitos de Tributos Municipais (Mobiliários);
 - v. Certidão Negativa de Débitos Trabalhistas (CNDT);
 - vi. Certidão Negativa de Falência ou Recuperação Judicial.
- d) Responder por quaisquer danos, perdas ou prejuízos causados diretamente a CONTRATANTE ou a terceiros decorrentes da execução deste contrato;
- e) Dar ciência imediata e por escrito a CONTRATANTE de qualquer anormalidade que verificar na execução do contrato;



CO-05.06/2021

- f) Prestar a CONTRATANTE, por escrito, os esclarecimentos solicitados e atender prontamente as reclamações sobre a execução do contrato;
- g) Responder pelos encargos trabalhistas, previdenciários, fiscais, comerciais e tributários, resultantes da execução deste contrato, nos termos do artigo 77, da Lei Federal nº 13.303/16.

2.2. São obrigações da CONTRATANTE:

- a) Exercer a fiscalização do contrato, designando fiscal (is) pelo acompanhamento da execução contratual; procedendo ao registro das ocorrências e adotando as providências necessárias ao seu fiel cumprimento, tendo por parâmetro os resultados previstos no contrato
- b) Fornecer à CONTRATADA todos os dados e informações necessários à execução do contrato;
- c) Efetuar o pagamento devido, de acordo com o estabelecido neste contrato.;
- d) Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;
- e) Comunicar a CONTRATADA formalmente (por e-mail) todas e quaisquer ocorrências relacionadas com a prestação dos serviços objeto deste Termo de Referência;

CLÁUSULA III – VIGÊNCIA CONTRATUAL

3.1. O contrato terá vigência de 36 (trinta e seis) meses, a contar da data de assinatura do Termo de Aceite Final, previsto no item 16.1 do Termo de Referência, podendo ser prorrogado até o limite de 5 anos, conforme dispõe o artigo 71, da Lei Federal nº 13.303/16.

3.2. Qualquer alteração, prorrogação e/ou acréscimos no decorrer deste contrato será objeto de termo aditivo, previamente justificado e autorizado pela CONTRATANTE.

CLÁUSULA IV – PREÇO

4.1. A CONTRATANTE pagará a CONTRATADA os valores conforme tabela abaixo:

Item	Características	Quant.	Valor 12 meses	Valor 36 meses
1	Gerenciamento Integrado McAfee ePO (ePolicy Orchestrator) On Premises	1	R\$ 983,33	R\$ 2.950,00



prodam

CO-05.06/2021

2	Atualização das Licenças, Suporte e Manutenção da Suíte Antivírus McAfee MV2 – MVision Protect Plus contendo Antivírus ENS (Endpoint Security), Firewall for Endpoint, Web Control, Device Control, ATP (Adaptive Threat Protection), TIE (Threat Intelligence Exchange) e Application Control	37.000	R\$ 1.844.050,00	R\$ 5.532.150,00
3	Aquisição das novas Licenças, ATD (Advanced Threat Defense Appliance), incluindo suporte e manutenção	37.800	R\$ 420.000,00	R\$ 1.260.000,00
4	Atualização das Licenças, Suporte e Manutenção do MFE Move AV for Virtual Servers (Licenciado por Servidor Virtual)	800	R\$ 120.000,00	R\$ 360.000,00
5	Atualização da Licença, Suporte e Manutenção Licença MFE VirusScan for Storage para NAS	1	R\$ 3.300,00	R\$ 9.900,00
6	Aquisição das novas licenças, Suporte e Manutenção Licença MFE VirusScan for Storage para NAS	3	R\$ 25.000,00	R\$ 75.000,00
7	Suporte Especializado Enhanced Success Plan	1	R\$ 580.000,00	R\$ 1.740.000,00
8	Serviço de Suporte e Manutenção	1	R\$ 400.000,00	R\$ 1.200.000,00
9	Fornecimento de Servidores para aplicação, banco de dados e demais serviços, incluindo licenças, suporte e manutenção	5	R\$ 980.000,00	R\$ 2.940.000,00
VALOR TOTAL			R\$ 13.120.000,00	

4.1. O valor total do presente contrato é de **R\$ 13.120.000,00** (treze milhões, cento e vinte mil reais).

4.2. No valor acima já estão incluídos todos os tributos e encargos de qualquer espécie que incidam ou venham a incidir sobre o preço do presente contrato.

4.3. Resta vedado o reajuste do valor contratual por prazo inferior a 12 (doze) meses contados após um ano da data-limite para apresentação da proposta comercial ou do último reajuste, conforme disposto na **Lei Federal nº 10.192 de 14/10/2001**, ou, se novas normas federais sobre a matéria autorizarem o reajustamento antes deste prazo.



CO-05.06/2021

- 4.4. Após o período inicial de 12 (doze) meses de vigência, caso haja prorrogação, o contratado poderá ter seus preços reajustados, aplicando-se a variação do Índice de Preços ao Consumidor IPC/FIPE a contar da data da apresentação da proposta.
- 4.5. Deverá a CONTRATADA manifestar-se quanto ao reajuste do valor do contrato em, no máximo 10 (dez) dias úteis do vencimento do período de 12 (doze) meses, conforme item 4.4.

CLAUSULA V – CONDIÇÕES DE FATURAMENTO

- 5.1. O valor será faturado mensalmente (36 meses/parcelas), a partir da emissão do “TERMO DE ACEITE FINAL previsto no Item 16.1. do Termo de Referência. O encaminhamento da Nota Fiscal Eletrônica de Serviço deverá ser realizado através de Solicitação de Pagamento, a partir do 1º (primeiro) dia subsequente ao mês da efetiva prestação dos serviços e autorização do Gestor do Contrato.

CLÁUSULA VI – CONDIÇÕES DE PAGAMENTO

- 6.1. A Nota Fiscal Eletrônica de Serviço deverá ser emitida e encaminhada à CONTRATANTE, através do setor de Expediente, por meio do e-mail: gfl@prodam.sp.gov.br.
- 6.2. Após o recebimento da Nota Fiscal Eletrônica de Serviço, a CONTRATADA disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite de Pagamento, aprovando os serviços prestados.
- 6.3. O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pela Gerência de Planejamento e Controle Financeiro (GFP), em 30 (trinta) dias corridos a contar da data de emissão do Termo de Aceite de Pagamento.
- 6.4. Caso a Nota Fiscal Eletrônica de Serviço contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de Serviço, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE.
- 6.5. Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% “pro-rata tempore”), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.



CO-05.06/2021

CLÁUSULA VII – GARANTIA CONTRATUAL (Art. 70, §1º da Lei Federal nº 13.303/16)

7.1. A CONTRATADA deverá prestar garantia contratual no prazo máximo de 15 (quinze) dias a contar da assinatura do contrato, na forma do **artigo 70, § 1º da Lei Federal nº 13.303/16**, no valor de **R\$ 656.000,00 (seiscentos e cinquenta e seis mil reais)**, correspondente a 5% (cinco por cento) do valor contratado, observando os procedimentos a seguir elencados.

7.2. A garantia, qualquer que seja a modalidade escolhida, deverá abranger um período mínimo de três meses após o término da vigência contratual, devendo a garantia assegurar a cobertura de todos os eventos ocorridos durante a sua validade, ainda que o sinistro seja comunicado depois de expirada a vigência da contratação ou validade da garantia.

7.3. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

7.3.1. Prejuízos advindos do inadimplemento total ou parcial do objeto do contrato.

7.3.2. Prejuízos diretos causados à CONTRATANTE decorrentes de culpa ou dolo da CONTRATADA durante a execução do contrato.

7.3.3. Multas, moratórias e compensatórias, aplicadas pela CONTRATANTE.

7.3.4. Obrigações trabalhistas e previdenciárias relacionadas ao contrato e não adimplidas pela CONTRATADA.

7.4. A CONTRATADA deverá informar, expressamente, na apresentação da garantia, as formas de verificação de autenticidade e veracidade do referido documento junto às instituições responsáveis por sua emissão.

7.5. No caso de seguro-garantia, a instituição prestadora da garantia contratual deve ser devidamente autorizada pela Superintendência de Seguros Privados – SUSEP e, no caso de fiança bancária, pelo Banco Central do Brasil.

7.6. A insuficiência da garantia não desobriga a CONTRATADA quanto aos prejuízos por ela causados, responsabilizando-se por todas as perdas e danos apurados pela CONTRATANTE que sobejarem aquele valor.

7.7. Para cobrança pela CONTRATANTE de quaisquer valores da CONTRATADA, a qualquer título, a garantia poderá ser executada, a partir do 3º (terceiro) dia, contado da resposta NÃO CONHECIDA E/OU IMPROCEDENTE acerca da notificação judicial ou extrajudicial à CONTRATADA, na hipótese do não cumprimento de suas obrigações contratuais.

7.7.1. Se o valor da garantia for utilizado, total ou parcialmente, cobrança de penalidade aplicada ou pagamento de qualquer obrigação da CONTRATADA, deverá ser efetuada a reposição do valor no prazo de 15 (quinze) dias úteis, contados da data em que for notificada para fazê-lo.

7.8. Caso haja aditamento contratual que implique alteração do valor, a garantia oferecida deverá ser atualizada.



CO-05.06/2021

7.9. Não sendo a garantia executada por força de penalidade administrativa e não havendo débitos a saldar com a CONTRATANTE, a garantia prestada será devolvida ao término do contrato.

7.10. Quando prestada em dinheiro, a garantia será devolvida por meio de depósito em conta bancária e corrigida pelos índices da poupança, salvo na hipótese de aplicações de penalidades pecuniárias ou necessidade de ressarcimento de prejuízos causados pela CONTRATADA à CONTRATANTE ou a terceiros, hipóteses em que será restituído o saldo remanescente.

7.10.1. Na hipótese de garantia em dinheiro, a CONTRATADA deverá enviar uma cópia do depósito bancário para o e-mail contratosfornecedores@prodam.sp.gov.br, identificando o contrato e a que título foi realizado o depósito.

CLÁUSULA VIII – MATRIZ DE RISCOS

8.1. Tendo como premissa a obtenção do melhor custo contratual mediante a alocação do risco à parte com maior capacidade para geri-lo e absorvê-lo, as partes identificam os riscos decorrentes da presente relação contratual e, sem prejuízo de outras previsões contratuais, estabelecem os respectivos responsáveis na Matriz de Riscos constante no **ANEXO III** parte integrante deste contrato.

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

CLÁUSULA IX – CONFORMIDADE

9.1. A CONTRATADA, com relação às atividades, operações, serviços e trabalhos vinculados ao objeto do presente contrato, declara e garante o cumprimento dos dispositivos da Lei Anticorrupção – Lei 12.846/2013, e dos dispositivos 327, *caput*, § § 1º e 2º e 337-D do Código Penal Brasileiro

9.2. A CONTRATADA deverá defender, indenizar e manter a CONTRATANTE isenta de responsabilidade em relação a quaisquer reivindicações, danos, perdas, multas, custos e despesas, decorrentes ou relacionadas a qualquer descumprimento pela CONTRATADA das garantias e declarações previstas nesta cláusula e nas Leis Anticorrupção.

9.3. A CONTRATADA reportará, por escrito, para o endereço eletrônico ser fornecido oportunamente, qualquer solicitação, explícita ou implícita, de qualquer vantagem pessoal feita por empregado da CONTRATANTE para a CONTRATADA ou para qualquer membro da CONTRATADA, com relação às atividades, operações, serviços e trabalhos vinculados ao objeto do presente contrato.



prodam

CO-05.06/2021

9.4. Para a execução deste contrato, nenhuma das partes poderá oferecer, dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou não financeiras ou benefícios de qualquer espécie que constituam prática ilegal ou de corrupção, seja de forma direta ou indireta quanto ao objeto deste contrato, ou de outra forma a ele não relacionada, devendo garantir, ainda, que seus prepostos e colaboradores ajam da mesma forma, nos termos do Decreto n 56.633/2015.

9.5. O descumprimento das obrigações previstas nesta Cláusula poderá submeter à CONTRATADA à rescisão unilateral do contrato, a critério da CONTRATANTE, sem prejuízo da aplicação das sanções penais e administrativas cabíveis e, também, da instauração do processo administrativo de responsabilização de que tratam a Lei Federal nº 12.846/2013.

CLÁUSULA X – DA PROTEÇÃO DE DADOS

10.1. A **CONTRATADA** obriga-se, sempre que aplicável, a atuar no presente Contrato em conformidade com a legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, não colocando, por seus atos ou por omissão a **PRODAM-SP** em situação de violação das leis de privacidade, em especial, a Lei nº 13.709/2018 – Lei Geral de Dados Pessoais (“LGPD”).

10.2. Caso exista modificação dos textos legais acima indicados ou de qualquer outro, de forma que exija modificações na estrutura do escopo deste Contrato ou na execução das atividades ligadas a este Contrato, a **CONTRATADA** deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a **PRODAM-SP** poderá resolvê-lo sem qualquer penalidade, apurando-se os serviços prestados e/ou produtos fornecidos até a data da rescisão e conseqüentemente os valores devidos correspondentes.

10.3. A **CONTRATADA** se compromete a:

- i) Zelar pelo uso adequado dos dados aos quais venha a ter acesso, cuidando da sua integridade, confidencialidade e disponibilidade, bem como da infraestrutura de tecnologia da informação;
- ii) Seguir as instruções recebidas da **PRODAM-SP** em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, sob pena de arcar com as perdas e danos que eventualmente possa causar à **PRODAM**, aos seus colaboradores, clientes e fornecedores, sem prejuízo das demais sanções aplicáveis;
- iii) Responsabilizar-se, quando for o caso, pela anonimização dos dados fornecidos pela **PRODAM-SP**;
- iv) A **CONTRATADA** deverá notificar a **PRODAM-SP** em 24 (vinte e quatro) horas de (i) qualquer não cumprimento (ainda que suspeito) das obrigações legais relativas à proteção de Dados Pessoais; (ii) qualquer descumprimento das obrigações contratuais relativas ao tratamento dos Dados Pessoais; e (iii) qualquer violação de segurança no âmbito das atividades da **CONTRATADA**;

Empresa de Tecnologia da Informação e Comunicação do Município de São Paulo
Rua Líbero Badaró, 4525 - Centro - CEP: 01009-000 - São Paulo - SP
prodam.sp.gov.br | prodam@prodam.sp.gov.br



prodam

CO-05.06/2021

- v) A **CONTRATADA** deverá notificar a **PRODAM-SP** sobre quaisquer solicitações dos titulares de Dados Pessoais que venha a receber, como, por exemplo, mas não se limitando, a questões como correção, exclusão, complementação e bloqueio de dados, e sobre as ordens de tribunais, autoridade pública e regulamentadores competentes, e quaisquer outras exposições ou ameaças em relação à conformidade com a proteção de dados identificadas pelo mesmo;
- vi) A Contratada se compromete a manter sob todas as formas e meios, o sigilo de todas as informações e dados que, por algum motivo, tiver acesso, sob pena de responder judicialmente e administrativamente, ressaltando a LGPD, a qual deverá ser respeitada na guarda e manutenção das informações e dados a que tiver acesso; e
- vii) Auxiliar a **PRODAM-SP** com as suas obrigações judiciais ou administrativas aplicáveis, de acordo com a LGPD e outras leis de privacidade aplicáveis, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança.

10.4. A CONTRATADA deverá manter registro das operações de tratamento de Dados Pessoais que realizar, bem como implementar medidas técnicas e organizacionais necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado para o tratamento de Dados Pessoais é estruturado de forma a atender os requisitos de segurança, os padrões de boas práticas de governança e os princípios gerais previstos na legislação e nas demais normas regulamentares aplicáveis.

10.5. A PRODAM-SP terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da **CONTRATADA** com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição da responsabilidade que a **CONTRATADA** possui perante a LGPD e este Contrato.

10.6. A CONTRATADA declara conhecer e que irá seguir todas as políticas de segurança da informação e privacidade da **PRODAM-SP**, bem como realizará treinamentos internos de conscientização a fim de envidar os maiores esforços para evitar o vazamento de dados, seja por meio físico ou digital, acidental ou por meio de invasão de sistemas de software.

10.7. O presente Contrato não transfere a propriedade de quaisquer dados da **PRODAM-SP** ou dos clientes desta para a **CONTRATADA**.

10.8. A PRODAM-SP não autoriza a **CONTRATADA** a usar, compartilhar ou comercializar quaisquer eventuais elementos de dados, que se originem ou sejam criados a partir do tratamento de Dados Pessoais, estabelecido por este Contrato.



prodam

CO-05.06/2021

CLÁUSULA XI – SANÇÕES ADMINISTRATIVAS

11.1. A CONTRATADA está sujeita além das penalidades previstas na Lei Federal nº 13.303/16, sem prejuízo da apuração de perdas e danos, em especial:

- a) **Advertência por escrito;**
- b) **Multa de até 10% (dez por cento)** sobre o valor total do instrumento contratual ou da parcela correspondente, se o serviço prestado estiver em desacordo com as especificações contidas no **Termo de Referência – ANEXO I**;
- c) **Multa de 10% (dez por cento)** sobre o valor total do instrumento contratual no caso de rescisão, por culpa ou a requerimento da CONTRATADA, sem motivo justificado ou amparo legal;
- d) **Suspensão temporária** de participação em licitação e impedimento de contratar com a PRODAM-SP, pelo prazo de até 02 (dois) anos;
- e) **Multa de até 20% (vinte por cento)** sobre o valor total do instrumento contratual caso não haja a execução do contrato nos prazos estabelecidos.

11.2. Para a cobrança, pela CONTRATANTE, de quaisquer valores da CONTRATADA, a qualquer título, a garantia contratual poderá ser executada na forma da lei.

11.3. Previamente a aplicação de quaisquer penalidades a CONTRATADA será notificada pela CONTRATANTE a apresentar defesa prévia, no prazo de 10 (dez) dias conforme § 2º do art. 83 da Lei nº 13.303/2016, contados do recebimento da notificação que será enviada ao endereço constante do preâmbulo do Contrato.

11.4. Considera-se recebida a notificação na data da assinatura do aviso de recebimento ou, na ausência deste, a data constante na consulta de andamento de entrega realizada no site dos correios, sendo certificado nos autos do processo administrativo correspondente qualquer destas datas.

11.6.1. Caso haja recusa da CONTRATADA em receber a notificação, esta será considerada recebida na data da recusa, contando a partir desta data o prazo para interposição da defesa prévia.

11.5. A aplicação de penalidade de multa não impede a responsabilidade da CONTRATADA por perdas e danos decorrente de descumprimento total ou parcial do contrato.

11.6. A aplicação de quaisquer multas pecuniárias não implica renúncia, pela PRODAM, do direito ao ressarcimento dos prejuízos apurados e que sobejarem o valor das multas cobradas.



prodam

CO-05.06/2021

11.7. As decisões da Administração Pública referentes à efetiva aplicação da penalidade ou sua dispensa serão publicadas no Diário Oficial da Cidade de São Paulo, nos termos do Decreto Municipal nº 44.279/03, ressalvados os casos previstos no referido ato normativo – sendo certo que a aplicação das penalidades de advertência e multa se efetivará apenas pela publicação no referido Diário, desnecessária a intimação pessoal.

CLÁUSULA XII – RESCISÃO

12.1. A **PRODAM-SP** poderá rescindir o presente contrato, nos termos do artigo 473, do Código Civil, nas seguintes hipóteses:

- a) Inexecução total do contrato, incluindo a hipótese prevista no artigo 395, parágrafo único do Código Civil;
- b) Atraso injustificado no início do serviço;
- c) Paralisação do serviço, sem justa causa e prévia comunicação à PRODAM-SP;
- d) Cometimento reiterado de faltas na sua execução que impeçam o prosseguimento do contrato;
- e) Transferência, no todo ou em parte, deste contrato, sem prévia e expressa autorização da CONTRATANTE;
- f) Decretação de falência;
- g) Dissolução da sociedade;
- h) Descumprimento do disposto no inciso XXXIII do artigo 7º da Constituição Federal, que proíbe o trabalho noturno, perigoso ou insalubre a menores de 18 anos e qualquer trabalho a menores de 16 anos, salvo na condição de aprendiz, a partir de 14 anos;
- i) Prática pela CONTRATADA de atos lesivos à Administração Pública previstos na Lei nº 8.429/1992 (Lei de Improbidade Administrativa) e Lei nº 12.846/2013 (Lei Anticorrupção);
- j) Prática de atos que prejudiquem ou comprometam a imagem ou reputação da PRODAM, direta ou indiretamente;

12.1.1. A rescisão a que se refere esta cláusula, deverá ser precedida de comunicação escrita e fundamentada da parte interessada e ser enviada à outra parte com antecedência mínima de 10 (dez) dias.

12.2. Desde que haja conveniência para a **PRODAM-SP**, a rescisão amigável é possível, por acordo entre as partes devidamente reduzido a termo no competente processo administrativo.

12.3. Poderá haver também rescisão por determinação judicial nos casos previstos pela legislação.

12.4. A rescisão administrativa ou amigável deverá ser precedida de autorização escrita e fundamentada da autoridade competente.



CO-05.06/2021

12.5. Não constituem causas de rescisão contratual o não cumprimento das obrigações aqui assumidas em decorrência dos fatos que independam da vontade das partes, tais como os que configurem caso fortuito e força maior, previstos no artigo 393, do Código Civil.

12.6. Os efeitos da rescisão do contrato serão operados a partir da comunicação escrita, ou, na impossibilidade de notificação do interessado, por meio de publicação oficial; ou da decisão judicial, se for o caso.

CLÁUSULA XIII – DISPOSIÇÕES GERAIS

13.1. Os termos e disposições deste contrato prevalecerão sobre quaisquer outros entendimentos ou acordos anteriores entre as partes, explícitos ou implícitos, referentes às condições nele estabelecidas.

13.1.1. O presente instrumento e suas cláusulas se regulam pela Lei Federal nº 13.303/16, pelos preceitos de direito privado, mormente a Lei n. 10.406/02 (Código Civil) e disposições contidas na legislação municipal, no que couber.

13.2. A CONTRATADA deverá, sob pena de rejeição, indicar o número deste contrato do **Edital do Pregão Eletrônico nº 05.002/2021** nas faturas pertinentes, que deverão ser preenchidas com clareza, por meios eletrônicos, à máquina ou em letra de forma.

13.3. A inadimplência do contratado quanto aos encargos trabalhistas, fiscais e comerciais não transfere à empresa pública ou à sociedade de economia mista a responsabilidade por seu pagamento, nem poderá onerar o objeto do contrato ou restringir a regularização e o uso das obras e edificações, inclusive perante o Registro de Imóveis.

13.4. A mera tolerância do descumprimento de qualquer obrigação não implicará perdão, renúncia, novação ou alteração do pactuado.

13.5. Na hipótese de ocorrência de fatos imprevisíveis que reflitam nos preços dos serviços, tornando-o inexecutável, poderão as partes proceder a revisão dos mesmos, de acordo com o disposto no artigo 81, § 5º, da Lei Federal nº 13.303/16.

13.6. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e o CONTRATANTE, vedando-se qualquer relação entre estes que caracterize personalidade e subordinação direta.

CLÁUSULA XIV – VINCULAÇÃO AO EDITAL

14.1. O cumprimento deste contrato está vinculado aos termos do **Edital do Pregão Eletrônico nº PE-05.002/2021** e seus anexos e à proposta da Contratada (doc. SEI 045620347).



prodam

CO-05.06/2021

CLÁUSULA XV – FORO

15.1. As partes elegem o Foro Cível da Comarca da Capital de São Paulo, com renúncia de qualquer outro, por mais privilegiado que seja, para dirimir quaisquer dúvidas que possam surgir no decorrer da execução deste contrato.

E por estarem assim, justas e contratadas, assinam as partes o presente instrumento em 2 (duas) vias de igual teor, perante 2 (duas) testemunhas abaixo.

São Paulo/SP, 8 de junho de 2021.

CONTRATANTE:

JORGE PEREIRA LEITE
Diretor de Administração e Finanças

ALEXANDRE GEDANKEN
Diretor de Infraestrutura e Tecnologia

CONTRATADA:

RENATO TENÓRIO
Procurador

Renato Tenório
Diretor Executivo
RG.: 19.953.787-2
ISH TECNOLOGIA S.A.

TESTEMUNHAS:

1. **JOSÉ NILDO GUERRA DIAS**
RG 22.667.682-1
CPF 128.497.858-30

2. **Satiana Rosa mie Kusano**
RG: 32.701.227-4



prodam

CO-05.06/2021

ANEXO I

TERMO DE REFERÊNCIA

1. Objeto

Contratação de empresa especializada em fornecimento de atualizações de licenças de uso para 37.000 licenças da Suíte Antivírus McAfee MV2 – Mvision Protect Plus contendo Antivírus ENS (Endpoint Security), Firewall for Endpoint, Web Control, Device Control, ATP (Adaptive Threat Protection), TIE (Threat Intelligence Exchange), Application Control, ePO On Premises, 800 licenças de MFE Move AV For Virtual Servers, 1 licença MFE VirusScan for Storage para NAS, fornecimento de novas licenças para 37.800 ATD (Advanced Threat Defense Appliance), 3 licenças MFE VirusCan for Storage para NAS, fornecimento de 5 servidores para aplicação e banco de dados, Suporte Especializado Enhanced Success Plan e Serviço de Suporte e Manutenção para toda a solução, pelo prazo de 36 meses.

2. Tabela de Composição de Itens:



CO-05.06/2021

Item	Características	Qtde.
1	Gerenciamento Integrado McAfee ePO (ePolicy Orchestrator) On Premises	1
2	Atualização das Licenças, Suporte e Manutenção da Suíte Antivírus McAfee MV2 – Mvision Protect Plus contendo Antivírus ENS (Endpoint Security), Firewall for Endpoint, Web Control, Device Control, ATP (Adaptive Threat Protection), TIE (Threat Intelligence Exchange) e Application Control	37.000
3	Aquisição das novas Licenças, ATD (Advanced Threat Defense Appliance), incluindo suporte e manutenção	37.800
4	Atualização das Licenças, Suporte e Manutenção do MFE Move AV for Virtual Servers (Licenciado por Servidor Virtual)	800
5	Atualização da Licença, Suporte e Manutenção Licença MFE VirusScan for Storage para NAS	1
6	Aquisição das novas licenças, Suporte e Manutenção Licença MFE VirusScan for Storage para NAS	3
7	Suporte Especializado Enhanced Success Plan	1
8	Serviço de Suporte e Manutenção	1
9	Fornecimento de Servidores para aplicação, banco de dados e demais serviços, incluindo licenças, suporte e manutenção	5



CO-05.06/2021

3. Especificação Técnica

3.1. Suíte McAfee ePolicy Orchestrator e Banco de Dados SQL Server

3.1.1. Licenças da Suíte McAfee ePolicy Orchestrator for Endpoint

3.1.2. **Quantidades**

3.1.2.1. 2 (dois) Servidores físicos para instalação On Premises do ePO e do Banco de Dados SQL Server;

3.1.2.2. 1 (uma) Licença de subscrição incluindo suporte e atualizações;

3.1.3. **Especificação Técnica dos Servidores ePolicy Orchestrator e o Banco de Dados**

3.1.3.1. Deve ser disponibilizada uma solução de Gerenciamento centralizada para estações de trabalho e servidores, do mesmo fabricante, instalada em um único servidor de aplicação, a fim de prover um único ponto de gerenciamento centralizado pela CONTRATANTE nesta contratação ou futura;

3.1.3.2. Toda infraestrutura necessária para gerenciamento da solução de antivírus, como servidores, sistemas operacionais, banco de dados, entre outros serviços e equipamentos necessários, deve ser disponibilizado em nosso datacenter pelo CONTRATADO com as devidas licenças para seu pleno funcionamento;

3.1.3.3. Deve ser apresentado um projeto de implantação em até 60 dias corridos após a assinatura do contrato de toda a solução de antivírus, bem como o gerenciamento e banco de dados, definidos por etapas:

3.1.3.3.1. Entrega dos servidores de aplicação e banco de dados;

3.1.3.3.2. Entrega das licenças de softwares dos servidores e banco de dados;

3.1.3.3.3. Instalação do gerenciamento centralizado;

3.1.3.3.4. Configuração do bando de dados;

3.1.3.3.5. Definição das regras e políticas de implantação;

3.1.3.3.6. Definição dos produtos contratados e configurados no ePO;

3.1.3.3.7. Definição da implantação dos appliance do ATD;

3.1.3.3.8. Definição de como será feito a instalação do agente do antivírus;

3.1.3.3.9. Prazo de cada implantação;

3.1.3.4. A administração deve estar acessível através de HTTPS utilizando-se de um dos navegadores abaixo ou aplicação do fabricante:

3.1.3.4.1. Google Chrome;

3.1.3.4.2. Edge;

3.1.3.4.3. Firefox.



CO-05.06/2021

- 3.1.3.5. A solução de gerenciamento On Premises, o serviço de Gerenciamento deve permitir a instalação em modo centralizado ou em modo descentralizado, permitindo que localidades remotas possuam um servidor local;
- 3.1.3.6. O servidor de gerenciamento deve suportar a instalação nos seguintes sistemas operacionais:
 - 3.1.3.6.1. Windows Server 2016;
 - 3.1.3.6.2. Windows Server 2019;
 - 3.1.3.6.3. A arquitetura dos Sistemas Operacionais deve ser 64-bits.
- 3.1.3.7. Deve suportar a instalação em Cluster Microsoft;
- 3.1.3.8. Deve suportar Ipv4 e Ipv6;
- 3.1.3.9. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:
 - 3.1.3.9.1. Vmware ESX;
 - 3.1.3.9.2. Citrix Xen Server;
 - 3.1.3.9.3. Microsoft Hyper-V.
- 3.1.3.10. O Servidor de Banco de dados deve possuir a instalação do SQL Server na versão recomendada pela McAfee durante todo o contrato;
 - 3.1.3.10.1. SQL Server 2019 ou superior;
 - 3.1.3.10.2. Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas.
- 3.1.3.11. O tamanho do banco de dados deve suportar 6 meses de retenção de logs do gerenciamento de antivírus;
- 3.1.3.12. Deve ser possível agregar a instalação da solução em:
 - 3.1.3.12.1. Servidor Console Central;
 - 3.1.3.12.2. Servidor Base de Dados;
 - 3.1.3.12.3. Servidor de Interação com os Agentes;
 - 3.1.3.12.4. Agentes Distribuidores de Vacina.
- 3.1.3.13. Deve suportar o uso do SQL Server em ambientes SAN;
- 3.1.4. **Console de Gerência McAfee ePolicy Orchestrator**
 - 3.1.4.1. Gerência centralizada e integrada, a partir de uma única console, para as ferramentas integradas de segurança em estações de trabalho e servidores, de onde seja possível manter a proteção atualizada, gerar relatórios, visualizar eventos e gerenciar políticas;
 - 3.1.4.2. Deve possuir um menu que possibilite ao administrador visualizar as funcionalidades de:
 - 3.1.4.2.1. Gerência de Relatórios;
 - 3.1.4.2.2. Gerência de Sistemas;
 - 3.1.4.2.3. Gerência de Políticas e configurações dos produtos listados neste termo de referência;
 - 3.1.4.2.4. Gerência de Softwares;
 - 3.1.4.2.5. Gerência de Automação;
 - 3.1.4.2.6. Gerência de Usuários;



prodam

CO-05.06/2021

- 3.1.4.2.7. Gerência de Configuração;
- 3.1.4.3. Deve apresentar aos administradores as páginas de Menu acessadas mais recentes;
- 3.1.4.4. Deve possibilitar ao administrador a visibilidade do ambiente por meio de Dashboards existentes na solução;
- 3.1.4.5. Deve permitir ao administrador a criação, edição, importação e exportação de dashboards;
- 3.1.4.6. Ao criar um dashboard:
 - 3.1.4.6.1. O administrador deve escolher entre mantê-lo:
 - 3.1.4.6.1.1. Privado;
 - 3.1.4.6.1.2. Público;
 - 3.1.4.6.1.3. Compartilhado;
 - 3.1.4.6.2. Deve permitir a criação de novos dashboards utilizando:
 - 3.1.4.6.2.1. Informação de Gerência de Sistemas;
 - 3.1.4.6.2.2. Informação de Eventos;
 - 3.1.4.6.2.3. Informação de Gestão de Políticas;
 - 3.1.4.6.2.4. Informação de Sistemas Detectados;
 - 3.1.4.6.2.5. Informação do módulo Endpoint Security;
 - 3.1.4.6.2.6. Informação de estatística do agente;
 - 3.1.4.6.2.7. Informação de log;
 - 3.1.4.6.3. Durante a criação de um novo dashboard, a ferramenta deverá permitir a escolha de:
 - 3.1.4.6.3.1. Tipo de Informação;
 - 3.1.4.6.3.2. Tipo de Gráfico;
 - 3.1.4.6.3.3. Tipo de dados que serão apresentados;
 - 3.1.4.6.3.4. Tipo de Filtros;
- 3.1.4.7. A solução deve apresentar a query SQL realizada para a apresentação de um dashboard;
 - 3.1.4.7.1. Deve permitir a exportação dos dados apresentados em um dashboard contendo apenas um sumário executivo ou o sumário mais a coleta completa;
 - 3.1.4.7.2. Deve permitir exportar o dashboard nos formatos CSV, XML, HTML e PDF;
 - 3.1.4.7.3. Deve permitir ao administrador a criação de relatórios, por meio de uma ferramenta integrada a console de administração, permitindo a customização do formato do relatório;
 - 3.1.4.7.4. Deve possibilitar ao administrador o uso de queries já criadas para a construção de relatórios;
 - 3.1.4.7.5. Deve possuir painel gráfico específico para o monitoramento dos eventos de:
 - 3.1.4.7.5.1. Regras de Firewall;
 - 3.1.4.7.5.2. Log de evento de ameaças;
 - 3.1.4.7.5.3. Eventos de prevenção de exploração;



prodam

CO-05.06/2021

- 3.1.4.7.5.4. Evento da solução de aprendizado de máquina;
- 3.1.4.8. Permitir a instalação dos Módulos da Solução a partir de um único servidor:
 - 3.1.4.8.1. A solução deverá permitir a instalação do agente de maneira facilitada, dentre elas:
 - 3.1.4.8.1.1. Criação de uma URL com o instalador;
 - 3.1.4.8.1.2. Criação de um pacote de instalação;
 - 3.1.4.8.1.3. Integração por meio do Active Directory;
 - 3.1.4.9. Resposta automática ao detectar uma nova máquina sem agente da solução;
 - 3.1.4.10. Ao instalar o novo agente, o mesmo deve ser redirecionado, de maneira automática, ao grupo pertencente;
 - 3.1.4.11. A criação de grupos deve ser customizada ou por meio de integração com serviços de diretório (Exemplo: Active Directory);
 - 3.1.4.12. A ordenação de cliente deve obedecer a regras pré-estabelecidas pelo administrador da solução, sendo no mínimo:
 - 3.1.4.12.1. Endereço IP;
 - 3.1.4.13. A ordenação por meio do uso do Endereçamento IP, deve permitir o uso de um único endereço, um range IPV4/IPV6 e sub redes;
 - 3.1.4.13.1. Marcação:
 - 3.1.4.13.1.1. A ordenação por meio do uso de Marcadores, deve ser possível por meio da seleção de propriedades, dentre elas:
 - 3.1.4.13.1.1.1. Tipo de CPU;
 - 3.1.4.13.1.1.2. Nome DNS;
 - 3.1.4.13.1.1.3. Memória Livre;
 - 3.1.4.13.1.1.4. Se é um Laptop;
 - 3.1.4.13.1.1.5. Endereço MAC;
 - 3.1.4.13.1.1.6. Descrição do Sistema;
 - 3.1.4.13.1.1.7. Plataforma do Sistema Operacional;
 - 3.1.4.13.1.1.8. Tipo do Sistema Operacional;
 - 3.1.4.13.1.1.9. Versão do Sistema Operacional;
 - 3.1.4.14. Para cada grupo, deve ser possível indicar a herança de política da raiz ou quebrar a herança e definir novos parâmetros;
 - 3.1.4.15. Deve permitir a visualização de tarefas especificadas para cada grupo;
 - 3.1.4.16. Deve permitir a visualização das políticas aplicadas para cada grupo;
 - 3.1.4.17. Para permitir a descoberta de máquinas sem agente, a solução deverá trabalhar com agentes sensores que identificam máquinas sem agente;



prodam

CO-05.06/2021

- 3.1.4.17.1. Ao identificar uma máquina sem agente, a solução deve permitir a criação de resposta automatizada, permitindo que a instalação seja feita de maneira silenciosa para o usuário e não assistida pelo administrador da solução;
- 3.1.4.17.2. Deve permitir a adição manual de sistemas não gerenciados, permitindo a posterior instalação do agente;
- 3.1.4.18. Permitir a alteração das políticas do Módulos da Solução nos clientes de maneira remota;
- 3.1.4.19. Deve permitir a alteração das políticas em um único agente;
- 3.1.4.20. Possuir a integração com o gerenciamento da solução de segurança de estações de trabalho e servidores, deste mesmo fabricante a fim de prover uma única console de gerenciamento centralizado de todas as soluções de segurança;
- 3.1.4.21. Permitir a atualização incremental da lista de definições de vírus nos clientes, a partir de um único ponto da rede local;
- 3.1.4.22. Deve possibilitar a configuração de melhor seleção do repositório por meio de:
 - 3.1.4.22.1. Menor tempo de ping;
 - 3.1.4.22.2. Distância de sub redes;
- 3.1.4.23. Deve permitir a criação de uma lista de repositórios que os clientes deverão buscar por ordem de prioridade;
- 3.1.4.24. Deve permitir a criação de um grupo de teste para a aplicação da vacina antes de espalhar para os demais agentes do ambiente, este processo deve ser automático;
- 3.1.4.25. A solução deve permitir o uso de repositórios distribuídos para a distribuição de softwares, vacinas e atualizações e patches;
- 3.1.4.26. Os repositórios distribuídos devem estar sincronizados com o repositório central;
- 3.1.4.27. Em caso de indisponibilidade do repositório central, deve ser possível a configuração de um repositório backup no qual os repositórios irão em busca de atualizações;
- 3.1.4.28. A adição de um novo repositório deve obedecer aos seguintes parâmetros:
 - 3.1.4.28.1. Tipo;
 - 3.1.4.28.2. HTTP;
 - 3.1.4.28.3. FTP;
 - 3.1.4.28.4. UNC;
 - 3.1.4.28.5. Servidor Remoto;
 - 3.1.4.28.6. Credenciais;
 - 3.1.4.28.7. Atualizações;
- 3.1.4.29. Deve permitir a criação de agentes locais com privilégios de distribuição de atualizações;



prodam

CO-05.06/2021

- 3.1.4.30. Deve possuir funcionalidade “lazy caching”, ou seja, fazer o download do repositório principal, apenas quando solicitado por algum outro agente;
- 3.1.4.31. A solução deverá permitir a instalação de agentes de replicação adicionais, responsáveis pela comunicação entre agente servidor, possibilitando a entrega de políticas e atualizações da solução;
- 3.1.4.32. Deve permitir a instalação de agentes de replicação na DMZ;
- 3.1.4.33. Deve possibilitar ao administrador a visualização das características básicas de hardware das máquinas, dentre elas:
 - 3.1.4.33.1. Informações de CPU;
 - 3.1.4.33.2. Informações de Memória;
 - 3.1.4.33.3. Informação de Disco;
 - 3.1.4.33.4. Nome DNS;
 - 3.1.4.33.5. Nome do Domínio;
 - 3.1.4.33.6. Endereço IP;
 - 3.1.4.33.7. Informações do Sistema Operacional;
 - 3.1.4.33.8. Time Zone;
 - 3.1.4.33.9. Usuário Logado;
 - 3.1.4.33.10. Se é VDI;
- 3.1.4.34. Deve permitir a criação de propriedades customizadas, a exemplo informar o modelo da placa de vídeo em uma propriedade customizada;
- 3.1.4.35. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados centralizado;
- 3.1.4.36. Permitir diferentes níveis de administração do servidor, de maneira independente do login da rede;
- 3.1.4.37. Deve permitir a criação de políticas customizadas;
- 3.1.4.38. Deve apresentar ao administrador um histórico de alteração de política para cada um dos módulos da solução, incluindo:
 - 3.1.4.38.1. Data;
 - 3.1.4.38.2. Usuário;
 - 3.1.4.38.3. Comentário;
 - 3.1.4.38.4. Versão do produto;
- 3.1.4.39. Deve criar regras de aplicação de política automatizada com base na estação de trabalho ou no usuário:
 - 3.1.4.39.1. Para a política baseada em usuários, deve ser possível criar, no mínimo, políticas diferenciadas para os módulos de Firewall de host e Filtro Web;
- 3.1.4.40. Deve permitir a criação de resposta automatizada ao detectar evento de ameaça, ou de cliente ou de servidor;
- 3.1.4.41. Dentre as ações de resposta automatizada, deve ser possível:
 - 3.1.4.41.1. Encaminhar uma Trap SNMP com o nome da ameaça, Severidade e a ação tomada;



prodam

CO-05.06/2021

- 3.1.4.41.2. Executar um comando do sistema;
- 3.1.4.41.3. Encaminhar um e-mail;
- 3.1.4.41.4. Uma tarefa do servidor;
- 3.1.4.41.5. Executar um comando externo;
- 3.1.4.42. Suporte a múltiplos usuários, com diferentes níveis de acesso e permissões aos produtos gerenciados;
- 3.1.4.43. Forçar a configuração determinada no servidor para os clientes;
- 3.1.4.44. Caso o cliente altere a configuração, a mesma deverá retornar ao padrão estabelecido no servidor, quando a mesma for verificada pelo agente;
- 3.1.4.45. A comunicação entre as máquinas clientes e o servidor de gerenciamento deve ser segura;
- 3.1.4.46. Geração de relatórios que contenham as seguintes informações:
 - 3.1.4.46.1. Máquinas com a lista de definições de vírus desatualizada;
 - 3.1.4.46.2. Qual a versão do software (inclusive versão gerenciada pela nuvem) instalado em cada máquina;
 - 3.1.4.46.3. Os vírus que mais foram detectados;
 - 3.1.4.46.4. As máquinas que mais sofreram infecções em um determinado período;
 - 3.1.4.46.5. Os usuários que mais sofreram infecções em um determinado período;
- 3.1.4.47. Deve ser capaz de identificar e apresentar uma visibilidade sobre quais estações executaram um determinado arquivo (executável);
- 3.1.4.48. Deve ser capaz de identificar o arquivo e bloqueá-lo baseado na reputação e em critério de risco;
- 3.1.4.49. Estes dashboards devem conter no mínimo todos os seguintes relatórios de fácil visualização:
 - 3.1.4.49.1. Cobertura da proteção de Navegação Segura;
 - 3.1.4.49.2. Relatório dos últimos 30 dias da detecção de códigos maliciosos;
 - 3.1.4.49.3. Top 10 Computadores com Infecções;
 - 3.1.4.49.4. Top 10 Computadores com Sites bloqueados pela política;
 - 3.1.4.49.5. Resumo das ações tomadas nos últimos 30 dias no que se refere a Filtro de Navegação na web;
 - 3.1.4.49.6. Resumo dos tipos de sites acessados nos últimos 30 dias no que se refere a Filtro de Navegação Segura;
- 3.1.4.50. Gerenciar a atualização do antivírus em computadores portáteis (notebooks), automaticamente, mediante conexão em rede local ou remota;
- 3.1.4.51. Suportar o uso de múltiplos repositórios para atualização de produtos e arquivo de vacina com replicação seletiva;
- 3.1.4.52. Ter a capacidade de gerar registros/logs para auditoria;



prodam

CO-05.06/2021

- 3.1.4.53. A solução de gerenciamento deve ter a capacidade de atribuir etiquetas as máquinas, facilitando assim a distribuição automática dentro dos grupos hierárquicos na estrutura de gerenciamento;
- 3.1.4.54. A gerência deve ser centralizada e suportar a gestão de todos os módulos listados neste Termo de Referência;
- 3.1.4.55. Não serão aceitas soluções que possuam mais de uma console de gestão;
- 3.1.4.56. Deve suportar a instalação nos seguintes sistemas operacionais:
 - 3.1.4.56.1. Windows Server 2012 Release 2;
 - 3.1.4.56.2. Windows Server 2012;
 - 3.1.4.56.3. Windows Server 2008 R2;
 - 3.1.4.56.4. Microsoft Windows Server 2016;
 - 3.1.4.56.5. Microsoft Windows Server 2019;
- 3.1.4.57. Deve suportar a instalação em Cluster Microsoft;
- 3.1.4.58. Deve suportar Ipv4 e Ipv6;
- 3.1.4.59. Deve suportar a virtualização do sistema operacional com base nos seguintes hypervisors:
 - 3.1.4.59.1. Vmware ESX;
 - 3.1.4.59.2. Citrix Xen Server;
 - 3.1.4.59.3. Microsoft Hyper-V;
- 3.1.4.60. Deve possuir suporte a base de dados:
 - 3.1.4.60.1. SQL Server 2012 ou superior;
 - 3.1.4.60.2. Não serão aceitas soluções que usam SQL Express ou Base de dados embutidas;
 - 3.1.4.60.3. A console deve ser acessível por meio dos principais browsers disponíveis no mercado por meio de conexão segura (Https):
 - 3.1.4.60.4. Google Chrome
 - 3.1.4.60.5. Mozilla Firefox
 - 3.1.4.60.6. Edge;
 - 3.1.4.61. Deve ser possível segregar a instalação da solução em:
 - 3.1.4.61.1. Servidor Console Central;
 - 3.1.4.61.2. Servidor Base de Dados;
 - 3.1.4.61.3. Servidor de Interação com os Agentes;
 - 3.1.4.61.4. Agentes Distribuidores de Vacina;

4. Suíte Antivirus McAfee MV2 – Mvision Protect Plus

4.1. Quantidades: 37.000

- 4.1.1. Atualização das subscrições, suporte e manutenção da Suíte McAfee MV2 – Mvision Protect Plus contendo:



prodam

CO-05.06/2021

- 4.1.1.1. Antivírus ENS (Endpoint Security);
- 4.1.1.2. Firewall for Endpoint;
- 4.1.1.3. Web Control;
- 4.1.1.4. Device Control;
- 4.1.1.5. Application Control;
- 4.1.1.6. ATP (Adaptive Threat Protection);
- 4.1.1.7. TIE (Threat Intelligence Exchange);

4.1.2. As licenças de subscrição incluindo suporte, manutenção e atualizações por 36 meses;

4.2. **Suíte McAfee Antivírus ENS (Endpoint Security)**

4.2.1.1. **Especificação Técnica:**

4.2.1.1.1. Deve possuir suporte às arquiteturas 32-bits e 64-bits;

4.2.1.1.2. Deve suportar as seguintes plataformas clientes:

- 4.2.1.1.2.1. Windows 10;
- 4.2.1.1.2.2. Windows 8.1;
- 4.2.1.1.2.3. Windows 8;
- 4.2.1.1.2.4. Windows 7;
- 4.2.1.1.2.5. Windows Server 2016;
- 4.2.1.1.2.6. Windows Server 2012;
- 4.2.1.1.2.7. Windows Server 2008 R2;
- 4.2.1.1.2.8. High Sierra 10.13.x
- 4.2.1.1.2.9. Sierra 10.12.x
- 4.2.1.1.2.10. El Captain 10.11.x
- 4.2.1.1.2.11. Yosemite 10.10.x
- 4.2.1.1.2.12. Sierra 10.12.x;
- 4.2.1.1.2.13. El Captain 10.11.x;
- 4.2.1.1.2.14. Yosemite 10.10.x;
- 4.2.1.1.2.15. Amazon Linux;
- 4.2.1.1.2.16. Red Hat Enterprise Linux
- 4.2.1.1.2.17. Suse Linux Enterprise
- 4.2.1.1.2.18. Oracle Linux
- 4.2.1.1.2.19. CentOS
- 4.2.1.1.2.20. Ubuntu
- 4.2.1.1.2.21. Debian
- 4.2.1.1.2.22. Fedora

4.2.1.1.3. Deve suportar a instalação de agente nos sistemas operacionais acima virtualizados nas seguintes plataformas:

- 4.2.1.1.4. AWS;
- 4.2.1.1.5. Azure;
- 4.2.1.1.6. Citrix XenApp;
- 4.2.1.1.7. Citrix XenDesktop;
- 4.2.1.1.8. Citrix XenServer;
- 4.2.1.1.9. Microsoft Hyper-V 2012 R2;



prodam

CO-05.06/2021

- 4.2.1.1.10. Vmware ESXi;
- 4.2.1.1.11. Vmware Player;
- 4.2.1.1.12. Vmware vShpere;
- 4.2.1.1.13. Vmware Workstation;
- 4.2.1.1.14. A proteção deverá ser realizada por softwares específicos que atendam a funcionalidades descritas neste termo e deverá conter um agente de gerenciamento independente dos softwares de proteção, permitindo que componentes sejam adicionados ou removidos conforme às necessidades dos administradores;
- 4.2.1.1.15. O conjunto de softwares de proteção e agente de gerenciamento deverão ser fornecidos pelo mesmo fabricante;
- 4.2.1.1.16. O software de proteção deve compreender as seguintes funcionalidades:
 - 4.2.1.1.16.1. Prevenção de ameaças;
 - 4.2.1.1.16.2. Firewall e prevenção contra intrusão;
 - 4.2.1.1.16.3. Controle Web;
 - 4.2.1.1.16.4. Prevenção adaptável contra ameaças;
- 4.2.1.1.17. Todas as funcionalidades deverão ser geridas por uma console única com as capacidades mínimas de:
 - 4.2.1.1.17.1. Relatórios;
 - 4.2.1.1.17.2. Dashboards;
 - 4.2.1.1.17.3. Políticas;
 - 4.2.1.1.17.4. Configuração;
 - 4.2.1.1.17.5. Instalação/Desinstalação;
- 4.2.1.1.18. O cliente deve ser capaz de operar em modo autônomo (self-managed) e permitir que as configurações sejam aplicadas diretamente no cliente;
- 4.2.1.1.19. O cliente deve ser capaz de atualizar as definições para detecção de ameaças, patches e hotfixes a partir de um servidor definido pelo administrador ou diretamente nos servidores do fabricante;
- 4.2.1.1.20. A solução de prevenção deve ser colaborativa, ou seja, os módulos exigidos devem ser capazes de trocarem informações para uma análise contextual, não baseada somente em assinaturas de detecção;
- 4.2.1.1.21. A solução deve possuir múltiplas camadas de proteção, não serão aceitas soluções baseadas apenas em assinaturas;
- 4.2.1.1.22. A solução deverá realizar verificações periódicas no ambiente para alertar o fabricante de potenciais problemas ocasionados pela atualização de vacina.



prodam

CO-05.06/2021

- 4.2.1.1.23. A solução deve conter módulo capaz de proteger contra redes de BOT, negação de serviço, executáveis não confiáveis e conexões web maliciosas;
- 4.2.1.1.24. A solução deve conter módulo capaz de garantir uma navegação web segura, prevenindo contra sites maliciosos, downloads de ameaças e garantir a política de acesso (Permitir/Negar)
- 4.2.1.1.25. A solução deve conter módulo capaz de garantir integração entre as soluções do fabricante proposto e entre soluções de fabricantes terceiros (Exemplo: Checkpoint, Fortinet, Avecto, TrapX, Fireeye, NMAP, Cisco, IBM), compartilhando as informações para melhor mitigar novas ameaças;
- 4.2.1.1.26. Este módulo deve estar público para o desenvolvimento da comunidade via Github;

4.2.1.2. Proteção Clientes Windows:

- 4.2.1.2.1. Prevenção de exploração:
 - 4.2.1.2.1.1. Deve ser possível selecionar no mínimo, dois modos de proteção (Padrão/Máximo);
- 4.2.1.2.2. Deve ser possível ativar/desativar a proteção contra escalonamento de privilégios genéricos;
- 4.2.1.2.3. Deve ser possível ativar/desativar a prevenção de execução de dados do Windows;
- 4.2.1.2.4. Deve ser possível selecionar dentre as ações de apenas bloquear ou apenas relatar ou bloquear e relatar;
- 4.2.1.2.5. Deve conter assinatura de ataques com conteúdo atualizável periodicamente;
- 4.2.1.2.6. Deve permitir aos administradores a criação de assinaturas personalizadas para controle de pastas, registro, processos, serviços;
- 4.2.1.2.7. Deve permitir o bloqueio de ameaças através de ataques de rede;
- 4.2.1.2.8. Deve permitir o monitoramento de ataques de Buffer Overflow em processos e aplicações específicas;
- 4.2.1.2.9. Deve ser possível incluir exclusões por:
 - 4.2.1.2.9.1. Processo;
 - 4.2.1.2.9.2. Nome;
 - 4.2.1.2.9.3. Caminho do arquivo;
 - 4.2.1.2.9.4. Hash MD5;
- 4.2.1.2.10. Módulo de chamada:
 - 4.2.1.2.10.1. Nome;
 - 4.2.1.2.10.2. Caminho;
 - 4.2.1.2.10.3. Hash MD5;
 - 4.2.1.2.10.4. Signatário Digital;



prodam

CO-05.06/2021

4.2.1.3. Proteção de acesso

4.2.1.3.1. Deve fornecer regras de proteção nativamente, ou seja, definidas pelo fabricante da solução, no mínimo, para:

- 4.2.1.3.1.1. Acesso remoto a pastas locais;
- 4.2.1.3.1.2. Alteração políticas de direitos dos usuários;
- 4.2.1.3.1.3. Alterar os registros de extensão dos arquivos;
- 4.2.1.3.1.4. Criação de novos arquivos na pasta Arquivo de Programas;
- 4.2.1.3.1.5. Criação de novos executáveis na pasta Windows;
- 4.2.1.3.1.6. Criar/Modificar remotamente arquivos Portable Executable, INI, PIF e as localizações do sistema;
- 4.2.1.3.1.7. Criar ou Modificar remotamente arquivos ou pastas;
- 4.2.1.3.1.8. Desativar o editor de registro e o gerenciador de tarefas;
- 4.2.1.3.1.9. Executar arquivos das pastas do usuário;
- 4.2.1.3.1.10. Execução de scripts pelo host de script do Windows;
- 4.2.1.3.1.11. Instalar objetos de ajuda a navegação ou extensões de shell;
- 4.2.1.3.1.12. Instalar novos CLSIDs, APPIDs e TYPEDLIBs;
- 4.2.1.3.1.13. Modificar configurações de rede;
- 4.2.1.3.1.14. Modificar configurações do Internet Explorer;
- 4.2.1.3.1.15. Modificar processos principais do Windows;
- 4.2.1.3.1.16. Navegadores iniciando programas da pasta de downloads;
- 4.2.1.3.1.17. Registrar programas para execução automática;

4.2.1.3.2. As regras especificadas devem permitir o seu:

- 4.2.1.3.2.1. Bloqueio, ou
- 4.2.1.3.2.2. Informação, ou
- 4.2.1.3.2.3. Bloqueio e Informação;

4.2.1.3.3. Deve permitir ao administrador criar regras de customizadas com no mínimo os seguintes parâmetros:

- 4.2.1.3.3.1. Processos;
- 4.2.1.3.3.2. Nome do processo;
- 4.2.1.3.3.3. Hash MD5;
- 4.2.1.3.3.4. Assinatura Digital;
- 4.2.1.3.3.5. Usuário

4.2.1.3.4. Arquivos, com as seguintes ações:

- 4.2.1.3.4.1. Criação;
- 4.2.1.3.4.2. Deletar;
- 4.2.1.3.4.3. Executar;
- 4.2.1.3.4.4. Alteração de permissão;
- 4.2.1.3.4.5. Leitura;



prodam

CO-05.06/2021

- 4.2.1.3.4.6. Renomear;
- 4.2.1.3.4.7. Escrever;
- 4.2.1.3.5. Chave de Registro, com as seguintes ações:
 - 4.2.1.3.5.1. Escrever;
 - 4.2.1.3.5.2. Criar;
 - 4.2.1.3.5.3. Deletar;
 - 4.2.1.3.5.4. Ler;
 - 4.2.1.3.5.5. Enumerar;
 - 4.2.1.3.5.6. Carregar;
 - 4.2.1.3.5.7. Substituir;
 - 4.2.1.3.5.8. Restaurar;
 - 4.2.1.3.5.9. Alterar permissão;
- 4.2.1.3.6. Valor de Registro, com as seguintes ações:
 - 4.2.1.3.6.1. Ler;
 - 4.2.1.3.6.2. Criar;
 - 4.2.1.3.6.3. Deletar;
- 4.2.1.3.7. Processos, com as seguintes ações:
 - 4.2.1.3.7.1. Qualquer acesso;
 - 4.2.1.3.7.2. Criar thread;
 - 4.2.1.3.7.3. Modificar;
 - 4.2.1.3.7.4. Terminar;
 - 4.2.1.3.7.5. Executar;
- 4.2.1.3.8. Serviços, com as seguintes ações:
 - 4.2.1.3.8.1. Iniciar;
 - 4.2.1.3.8.2. Interromper;
 - 4.2.1.3.8.3. Pausar;
 - 4.2.1.3.8.4. Continuar;
 - 4.2.1.3.8.5. Criar;
 - 4.2.1.3.8.6. Remover;
 - 4.2.1.3.8.7. Habilitar perfil de hardware;
 - 4.2.1.3.8.8. Desabilitar perfil de hardware;
 - 4.2.1.3.8.9. Alterar modo de inicialização;
 - 4.2.1.3.8.10. Alterar informação de logon;
 - 4.2.1.3.8.11. Deve permitir a criação de exclusões;

4.2.1.4. Varredura ao Acessar

- 4.2.1.4.1. A Varredura deve ser passível de habilitação/desativação por opção do administrador;
- 4.2.1.4.2. Deve iniciar a proteção durante a inicialização do sistema operacional;
- 4.2.1.4.3. Deve ser capaz de realizar análise no setor de boot;
- 4.2.1.4.4. O administrador da solução deve especificar o tempo máximo de análise para um único arquivo;
- 4.2.1.4.5. Deve analisar dos processos durante inicialização do serviço e na atualização de conteúdo;



prodam

CO-05.06/2021

- 4.2.1.4.6. Deve possibilitar ao administrador a análise de instaladores confiáveis;
- 4.2.1.4.7. Deve realizar análise durante cópia entre pastas locais;
- 4.2.1.4.8. A solução deve possuir conexão com Centro de Inteligência do fabricante, passível de ativação ou desativação por parte do administrador;
- 4.2.1.4.9. Deve permitir a configuração do nível de agressividade da análise entre:
 - 4.2.1.4.9.1. Muito Baixo;
 - 4.2.1.4.9.2. Baixo;
 - 4.2.1.4.9.3. Médio;
 - 4.2.1.4.9.4. Alto;
 - 4.2.1.4.9.5. Muito alto;
- 4.2.1.4.10. Deve conter integração com a funcionalidade AMSI (Antimalware Scan Interface) da Microsoft;
- 4.2.1.4.11. Deve possibilitar aplicar as configurações a todos os processos do sistema operacional ou a uma lista específica criada pelo administrador;
- 4.2.1.4.12. Deve realizar varredura quando o processo:
 - 4.2.1.4.12.1. Ler o disco;
 - 4.2.1.4.12.2. Gravar no disco;
 - 4.2.1.4.12.3. Deixar a solução de proteção decidir;
- 4.2.1.4.13. Deve possibilitar análise em:
 - 4.2.1.4.13.1. Unidades de Rede;
 - 4.2.1.4.13.2. Arquivos abertos para backup;
 - 4.2.1.4.13.3. Arquivos compactados, por exemplo .jar;
 - 4.2.1.4.13.4. Arquivos codificados (MIME)
- 4.2.1.4.14. Deve detectar programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;
- 4.2.1.4.15. Deve permitir a criação de perfis de varredura baseado em uma lista de processos;
- 4.2.1.4.16. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
 - 4.2.1.4.16.1. Limpar o arquivo;
 - 4.2.1.4.16.2. Excluir o arquivo;
 - 4.2.1.4.16.3. Negar acesso ao arquivo;
- 4.2.1.4.17. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
 - 4.2.1.4.17.1. Limpar o arquivo;
 - 4.2.1.4.17.2. Excluir o arquivo;
 - 4.2.1.4.17.3. Permitir acesso ao arquivo;
 - 4.2.1.4.17.4. Negar acesso ao arquivo;
- 4.2.1.4.18. Deve possibilitar ao administrador a gestão de uma lista de exclusões;



prodam

CO-05.06/2021

- 4.2.1.4.19. Deve possuir módulo capaz de interceptar scripts destinados ao Windows Host Scripting e analisá-lo para indicar se é malicioso ou não;
- 4.2.1.4.20. Deve permitir a criação de listas de exclusão de URL's que não sofrerão interceptação e análise de scripts;
- 4.2.1.4.21. Ao detectar uma ameaça o agente deverá emitir uma notificação ao usuário com uma mensagem a ser customizada pelo administrador da solução.

4.2.1.5. Varredura Sob Demanda

- 4.2.1.5.1. Deve ser possível realizar varreduras agendadas com periodicidade diária ou semanal;
- 4.2.1.5.2. Deve permitir a criação de repetição da tarefa;
- 4.2.1.5.3. Deve permitir definir a hora da execução da tarefa de análise;
- 4.2.1.5.4. Deve permitir a criação da tarefa de varredura de com agendamento aleatório;
- 4.2.1.5.5. Deve permitir a realização de varreduras agendadas após logon do usuário ou durante inicialização do sistema operacional;
- 4.2.1.5.6. Deve permitir escolher (um ou mais) os alvos da varredura, dentre eles:
 - 4.2.1.5.6.1. Os locais da varredura, dentre eles:
 - 4.2.1.5.6.1.1. Memória para rootkits;
 - 4.2.1.5.6.1.2. Processos em execução;
 - 4.2.1.5.6.1.3. Arquivos registrados;
 - 4.2.1.5.6.1.4. Meu computador;
 - 4.2.1.5.6.1.5. Todas as unidades locais;
 - 4.2.1.5.6.1.6. Todas as unidades fixas;
 - 4.2.1.5.6.1.7. Todas as unidades removíveis;
 - 4.2.1.5.6.1.8. Todas as unidades mapeadas;
 - 4.2.1.5.6.1.9. Pasta inicial;
 - 4.2.1.5.6.1.10. Pasta de perfil do usuário;
 - 4.2.1.5.6.1.11. Pasta Windows;
 - 4.2.1.5.6.1.12. Pasta de arquivos de programas;
 - 4.2.1.5.6.1.13. Pasta temporária;
 - 4.2.1.5.6.1.14. Lixeira;
 - 4.2.1.5.6.1.15. Arquivo ou pasta especificada pelo administrador;
 - 4.2.1.5.6.1.16. Setor de inicialização (boot);
 - 4.2.1.5.6.1.17. Arquivos compactados;
 - 4.2.1.5.6.1.18. Arquivos MIME;
- 4.2.1.5.7. Os tipos de arquivos que serão analisados;
- 4.2.1.5.8. Opções adicionais, como por exemplo detecção de programas indesejados, ameaças em programas desconhecidos e ameaças em macro desconhecidas;



prodam

CO-05.06/2021

- 4.2.1.5.9. Áreas de exclusão que não deverão ser varridas;
 - 4.2.1.5.10. Deve permitir a integração com o Centro de Inteligência do fabricante durante a varredura agendada para a detecção de ameaças desconhecidas;
 - 4.2.1.5.11. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar uma ameaça:
 - 4.2.1.5.11.1. Limpar o arquivo;
 - 4.2.1.5.11.2. Excluir o arquivo;
 - 4.2.1.5.11.3. Negar acesso ao arquivo;
 - 4.2.1.5.12. Deve permitir selecionar, no mínimo, uma das seguintes opções de ação após detectar um programa indesejado:
 - 4.2.1.5.12.1. Limpar o arquivo;
 - 4.2.1.5.12.2. Excluir o arquivo;
 - 4.2.1.5.12.3. Permitir acesso ao arquivo;
 - 4.2.1.5.12.4. Negar acesso ao arquivo;
 - 4.2.1.5.13. Para minimizar o impacto ao usuário, a solução deve permitir:
 - 4.2.1.5.13.1. Utilização de cache, ou seja, arquivos que já foram analisados e não tiveram seu conteúdo alterado não serão novamente analisados;
 - 4.2.1.5.13.2. Iniciar a varredura apenas quando o sistema estiver ocioso;
 - 4.2.1.5.14. Permitir ao usuário retomar varreduras pausadas;
 - 4.2.1.5.15. Deve permitir ao administrador inserir uma conta de domínio para realizar a análise de dispositivos de rede;
- 4.2.1.6. Proteção Clientes Linux**
- 4.2.1.6.1. Deve permitir a atualização automática das vacinas de detecção;
 - 4.2.1.6.2. Deve detectar ameaças usando métodos de acesso e de varredura sob demanda;
 - 4.2.1.6.3. Deve permitir a execução de varreduras por meio da console centralizada por meio de tarefas;
 - 4.2.1.6.4. Ao detectar uma ameaça, deverá responder com, no mínimo, as seguintes ações:
 - 4.2.1.6.4.1. Limpar o arquivo;
 - 4.2.1.6.4.2. Deletar o arquivo;
 - 4.2.1.6.4.3. Negar acesso ao arquivo;
 - 4.2.1.6.5. Deve possibilitar ao administrador, criar exceções de análise, ou seja, não permitir que a ferramenta execute uma análise em determinadas pastas ou arquivos;
 - 4.2.1.6.6. Deve permitir a opção de manter a configuração de exclusão realizada no agente, não sendo sobrescrita pela política principal;
 - 4.2.1.6.7. Deve permitir a gestão do agente local por meio de linha de comando;



prodam

CO-05.06/2021

- 4.2.1.6.8. Ao configurar a análise ao acessar, deve permitir:
 - 4.2.1.6.8.1. Quando analisar (exemplo: ao ler o arquivo)
 - 4.2.1.6.8.2. O que analisar (exemplo: todos os arquivos);
 - 4.2.1.6.9. Análise de arquivos comprimidos;
 - 4.2.1.6.10. Análise de volumes de rede;
 - 4.2.1.6.11. Análise de programas não desejados;
 - 4.2.1.6.12. Ao configurar a análise sob demanda, deve permitir:
 - 4.2.1.6.12.1. Análise de arquivos comprimidos;
 - 4.2.1.6.12.2. Análise de PUP;
 - 4.2.1.6.12.3. Análise de macros desconhecidos;
 - 4.2.1.6.12.4. Análise de programas desconhecidos;
 - 4.2.1.6.12.5. Caminhos da análise (path);
 - 4.2.1.6.12.6. Análise de pastas e subpastas;
 - 4.2.1.6.12.7. Análise de macros;
 - 4.2.1.6.12.8. Exclusão de paths, pastas e tipos de arquivos;
 - 4.2.1.6.12.9. Uso de cache;
 - 4.2.1.6.12.10. Ação Primária e Secundária;
 - 4.2.1.6.13. Deve possuir quarentena local para armazenar ameaças desconhecidas;
 - 4.2.1.6.14. Deve possuir ação para mover artefatos maliciosos para a área de quarentena;
 - 4.2.1.6.15. Deve usar heurística para detectar arquivos potencialmente maliciosos;
 - 4.2.1.6.16. Caso aconteça um timeout durante uma análise, deve permitir ao administrador a configuração de permitir ou negar o acesso ao arquivo;
- 4.2.1.7. McAfee Firewall for Endpoints**
- 4.2.1.7.1. O módulo de Firewall de Host deve incluir as seguintes capacidades:
 - 4.2.1.7.1.1. Deve permitir a ativação/desativação do módulo de Firewall através da console;
 - 4.2.1.7.1.2. Deve ser capaz de prevenir intrusões e proteger os nós gerenciados garantindo cobertura contra-ataques dia zero;
 - 4.2.1.7.1.3. Deve possuir um firewall de estação stateful bloqueando tráfego de entrada e controlando o tráfego de saída;
 - 4.2.1.7.1.4. Deve possuir assinaturas de proteção para:
 - 4.2.1.7.1.4.1. Arquivos;
 - 4.2.1.7.1.4.2. Chave de Registro;
 - 4.2.1.7.1.4.3. Processos;
 - 4.2.1.7.1.4.4. Serviços;
 - 4.2.1.7.1.5. Deve permitir o tráfego de saída somente após os serviços de Firewall estiverem iniciados;
 - 4.2.1.7.1.6. Deve ser possível bloquear trafego bridge;



prodam

CO-05.06/2021

- 4.2.1.7.1.7. Deve ser possível bloquear contra falsificação de IP (IP Spoofing);
- 4.2.1.7.2. O módulo deve permitir a criação de regras de maneira adaptativa, ou seja, em uma estação modelo definida pelo administrador deve ser capaz de criar as regras de maneira automática;
- 4.2.1.7.3. Deve ser possível bloquear o tráfego de todos os processos identificados como não confiáveis;
- 4.2.1.7.4. Deve permitir a criação de uma lista de processos identificados como confiáveis por meio das seguintes informações:
 - 4.2.1.7.4.1. Nome;
 - 4.2.1.7.4.2. Nome do arquivo ou Caminho;
 - 4.2.1.7.4.3. Hash MD5;
 - 4.2.1.7.4.4. Assinador digital;
- 4.2.1.7.5. Deve permitir integração com o Centro de Inteligência do próprio fabricante para bloqueio de ameaças advindas por meio de conexões maliciosas;
- 4.2.1.7.6. As conexões identificadas pelo Centro de Inteligência podem ser configuradas por meio de reputação mínima a ser bloqueada, por exemplo Risco Alto ou Risco Médio.
- 4.2.1.7.7. Deve ser possível registrar os eventos de conexões bloqueadas e permitidas pelo módulo;
- 4.2.1.7.8. Deve permitir inspeção do protocolo FTP;
- 4.2.1.7.9. Deve ser possível bloquear tráfego de protocolos não suportados;
- 4.2.1.7.10. O módulo de Firewall deve vir com um conjunto de regras previamente criadas pelo próprio fabricante.
- 4.2.1.7.11. O módulo de firewall deve permitir a criação de regras customizadas, com no mínimo os seguintes parâmetros:
 - 4.2.1.7.11.1. Ação:
 - 4.2.1.7.11.1.1. Bloquear;
 - 4.2.1.7.11.1.2. Permitir;
 - 4.2.1.7.11.2. Direção:
 - 4.2.1.7.11.2.1. Ambas;
 - 4.2.1.7.11.2.2. Entrada;
 - 4.2.1.7.11.2.3. Saída;
 - 4.2.1.7.11.3. Protocolo:
 - 4.2.1.7.11.3.1. Qualquer protocolo;
 - 4.2.1.7.11.3.2. Protocolo IP;
 - 4.2.1.7.11.3.3. Ipv4;
 - 4.2.1.7.11.3.4. Ipv6;
 - 4.2.1.7.11.3.5. Protocolo Não-IP 1.22.22.4;
 - 4.2.1.7.11.4. Tipo de Conexão:
 - 4.2.1.7.11.4.1. Rede Sem Fio;



prodam

CO-05.06/2021

- 4.2.1.7.11.4.2. Rede cabeada;
- 4.2.1.7.11.4.3. Rede Virtual;
- 4.2.1.7.11.5. Especificação da Rede:
 - 4.2.1.7.11.5.1. Endereço IP;
 - 4.2.1.7.11.5.2. Subnet;
 - 4.2.1.7.11.5.3. Range;
 - 4.2.1.7.11.5.4. FQDN;
- 4.2.1.7.11.6. Protocolo de Transporte:
 - 4.2.1.7.11.6.1. Todos;
 - 4.2.1.7.11.6.2. ICMP;
 - 4.2.1.7.11.6.3. ICMPv6
 - 4.2.1.7.11.6.4. TCP;
 - 4.2.1.7.11.6.5. UDP;
 - 4.2.1.7.11.6.6. STP;
 - 4.2.1.7.11.6.7. GRE;
 - 4.2.1.7.11.6.8. IGMP;
 - 4.2.1.7.11.6.9. IPSEC AH;
 - 4.2.1.7.11.6.10. IPSEC ESP;
 - 4.2.1.7.11.6.11. Ipv6 in Ipv4;
 - 4.2.1.7.11.6.12. over Ipv4;
 - 4.2.1.7.11.6.13. L2TP;
- 4.2.1.7.11.7. Agendamento:
 - 4.2.1.7.11.7.1. Dias da Semana;
 - 4.2.1.7.11.7.2. Hora Início;
 - 4.2.1.7.11.7.3. Hora Fim;
- 4.2.1.7.11.8. Aplicações:
 - 4.2.1.7.11.8.1. Deve possuir as seguintes proteções:
 - 4.2.1.7.11.8.1.1. Generic Buffer Overflow Protection;
 - 4.2.1.7.11.8.1.2. Suspicious caller and caller validation;
 - 4.2.1.7.11.8.1.3. Exploit Prevention;
 - 4.2.1.7.11.8.1.4. Data Execution Protection;
 - 4.2.1.7.11.8.1.5. Generic Privilege Escalation Protection;
 - 4.2.1.7.12. Deve possuir modulo de proteção contra intrusão por meio da rede;
 - 4.2.1.7.13. O módulo de proteção contra intrusos deve possuir regras já pré-definidas pelo fabricante;
 - 4.2.1.7.14. Deve permitir a criação customizada de regras de proteção, para no mínimo:
 - 4.2.1.7.14.1. Buffer Overflow;
 - 4.2.1.7.14.2. Uso ilegal de API;
 - 4.2.1.7.14.3. Arquivos;
 - 4.2.1.7.14.4. Serviços;
 - 4.2.1.7.14.5. Registro;



prodam

CO-05.06/2021

- 4.2.1.7.14.6. Processos;
- 4.2.1.7.14.7. Ao bloquear um determinado atacante pelo módulo de proteção de rede, deve ser possível indicar um tempo mínimo no qual a máquina atacante não poderá se comunicar com a atacada;
- 4.2.1.7.15. Deve permitir a indicação de assinaturas e endereços IP que não deverão ser levadas em consideração pelo mecanismo de análise;
- 4.2.1.7.16. Deverá possuir, no mínimo, as seguintes assinaturas:
 - 4.2.1.7.16.1. Proteção contra intrusão;
 - 4.2.1.7.16.2. TCP Port Scan;
 - 4.2.1.7.16.3. UDP Port Scan;
 - 4.2.1.7.16.4. Proteção contra vulnerabilidades SMB;
 - 4.2.1.7.16.5. Proteção contra brute force;
- 4.2.1.7.17. Serviços:
 - 4.2.1.7.17.1. IIS Envelope;
 - 4.2.1.7.17.2. IIS Shielding;
 - 4.2.1.7.17.3. MSSQL;
 - 4.2.1.7.17.4. Event Log;
 - 4.2.1.7.17.5. Remote Access;
 - 4.2.1.7.17.6. Netmon;
 - 4.2.1.7.17.7. Remote Command;
 - 4.2.1.7.17.8. RunAs;
 - 4.2.1.7.17.9. Registro;
 - 4.2.1.7.17.10. Drive usb inserido;
- 4.2.1.7.18. Processos:
 - 4.2.1.7.18.1. Double File Extension;
- 4.2.1.7.19. Buffer Overflow:
 - 4.2.1.7.19.1. Exchange;
 - 4.2.1.7.19.2. IIS;
 - 4.2.1.7.19.3. Services.exe;
 - 4.2.1.7.19.4. SVCHOST.exe;
 - 4.2.1.7.19.5. Generic Buffer Overflow;
 - 4.2.1.7.19.6. Generic Privilege Escalation;
 - 4.2.1.7.19.7. Windows Explorer;
 - 4.2.1.7.19.8. WinHLP32;
 - 4.2.1.7.19.9. Uso Ilegal de API;
 - 4.2.1.7.19.10. Mimikatz;
 - 4.2.1.7.19.11. MS Agent;
 - 4.2.1.7.19.12. Microsoft XML Core;
 - 4.2.1.7.19.13. Microsoft WMI Tools;
 - 4.2.1.7.19.14. MSDTC RPC Vulnerability;
 - 4.2.1.7.19.15. PowerShell Command Restriction;
 - 4.2.1.7.19.16. Print Spooler Load Library Vulnerability;
 - 4.2.1.7.19.17. Fileless Threat;



prodam

CO-05.06/2021

- 4.2.1.7.19.18. Firefox Illegal URL Quotes;
- 4.2.1.7.19.19. Google Desktop Javascript Injection;
- 4.2.1.7.19.20. Hidden Powershell;
- 4.2.1.7.20. Deve fornecer proteção para aplicações, constando na lista fornecida pelo fabricante, no mínimo:
 - 4.2.1.7.20.1. Adobe Acrobat;
 - 4.2.1.7.20.2. Adobe Flash Player;
 - 4.2.1.7.20.3. Adobe Flash Player Plugin;
 - 4.2.1.7.20.4. Apple iTunes;
 - 4.2.1.7.20.5. Apple Safari;
 - 4.2.1.7.20.6. CoolPDFReader;
 - 4.2.1.7.20.7. Cscript;
 - 4.2.1.7.20.8. Firefox;
 - 4.2.1.7.20.9. Google Chrome;
 - 4.2.1.7.20.10. Foxit Reader;
 - 4.2.1.7.20.11. Java Platform;
 - 4.2.1.7.20.12. Microsoft Edge;
 - 4.2.1.7.20.13. Microsoft Internet Explorer;
 - 4.2.1.7.20.14. Microsoft Outlook;
 - 4.2.1.7.20.15. Microsoft Visual C++;
 - 4.2.1.7.20.16. Microsoft Windows Explorer;
 - 4.2.1.7.20.17. Microsoft Windows Powershell;
 - 4.2.1.7.20.18. Microsoft Windows Win32 Runtime;
 - 4.2.1.7.20.19. Mozilla;
 - 4.2.1.7.20.20. OpenOffice;
 - 4.2.1.7.20.21. Registry Editor;
 - 4.2.1.7.20.22. VLC Media Player;

4.2.1.8. McAfee Web Control

- 4.2.1.8.1. Deve permitir o bloqueio de browsers não suportados, dentre eles:
 - 4.2.1.8.1.1. Opera;
 - 4.2.1.8.1.2. Safari for Windows;
 - 4.2.1.8.1.3. Netscape;
 - 4.2.1.8.1.4. Maxthon 1.23.1.5.Flock;
 - 4.2.1.8.1.5. Avant Browser;
 - 4.2.1.8.1.6. Deepnet Explorer;
 - 4.2.1.8.1.7. PhaseOut;
- 4.2.1.8.2. Deve permitir o controle de browsers suportados, dentre eles:
 - 4.2.1.8.2.1. Chrome;
 - 4.2.1.8.2.2. Firefox;
 - 4.2.1.8.2.3. Internet Explorer;
- 4.2.1.8.3. Deve ser capaz de utilizar lista de categorias para bloqueio de sites relacionados ao conteúdo não autorizado;
- 4.2.1.8.4. Deve possuir, no mínimo, as seguintes categorias:



prodam

CO-05.06/2021

- 4.2.1.8.4.1. Browser Exploits;
- 4.2.1.8.4.2. Download Maliciosos;
- 4.2.1.8.4.3. Sites Maliciosos;
- 4.2.1.8.4.4. Phishing;
- 4.2.1.8.4.5. Pornografia;
- 4.2.1.8.4.6. Hacking/Computer Crime;
- 4.2.1.8.4.7. Spyware/Adware/Keyloggers;
- 4.2.1.8.4.8. Anonymizer;
- 4.2.1.8.4.9. Anonymizer Utilities;
- 4.2.1.8.4.10. Alcohol;
- 4.2.1.8.4.11. Blogs/Wiki;
- 4.2.1.8.4.12. Business;
- 4.2.1.8.4.13. Chat;
- 4.2.1.8.4.14. Content Server;
- 4.2.1.8.4.15. Dating;
- 4.2.1.8.4.16. Dating/Social Networking;
- 4.2.1.8.4.17. Digital Postcards;
- 4.2.1.8.4.18. Discrimination;
- 4.2.1.8.4.19. Drugs;
- 4.2.1.8.4.20. Education;
- 4.2.1.8.4.21. Entertainment;
- 4.2.1.8.4.22. Extreme;
- 4.2.1.8.4.23. Fashion;
- 4.2.1.8.4.24. Finance;
- 4.2.1.8.4.25. For Kids;
- 4.2.1.8.4.26. Forum;
- 4.2.1.8.4.27. Gambling;
- 4.2.1.8.4.28. Game/Cartoon Violence;
- 4.2.1.8.4.29. Games;
- 4.2.1.8.4.30. General News;
- 4.2.1.8.4.31. Government/Military;
- 4.2.1.8.4.32. Gruesome Content;
- 4.2.1.8.4.33. Health;
- 4.2.1.8.4.34. Historical Revisionism;
- 4.2.1.8.4.35. History;
- 4.2.1.8.4.36. Humor/Comics;
- 4.2.1.8.4.37. Illegal UK;
- 4.2.1.8.4.38. Incidental Nudity;
- 4.2.1.8.4.39. Information Security;
- 4.2.1.8.4.40. Instant Messaging;
- 4.2.1.8.4.41. Interactive Web Applications;
- 4.2.1.8.4.42. Internet Rádio/TV;
- 4.2.1.8.4.43. Internet Services;
- 4.2.1.8.4.44. Job Search;
- 4.2.1.8.4.45. Major Global Religions;
- 4.2.1.8.4.46. Marketing/Merchandising;



prodam

CO-05.06/2021

- 4.2.1.8.4.47. Media Downloads;
- 4.2.1.8.4.48. Media Sharing;
- 4.2.1.8.4.49. Messaging;
- 4.2.1.8.4.50. Mobile Phone;
- 4.2.1.8.4.51. Moderated;
- 4.2.1.8.4.52. Motor Vehicles;
- 4.2.1.8.4.53. Non-Profit/Advocacy/NGO;
- 4.2.1.8.4.54. Nudity;
- 4.2.1.8.4.55. Online Shopping;
- 4.2.1.8.4.56. P2P/File Sharing;
- 4.2.1.8.4.57. Parked Domain;
- 4.2.1.8.4.58. Personal Network Storage;
- 4.2.1.8.4.59. Personal Pages;
- 4.2.1.8.4.60. Pharmacy;
- 4.2.1.8.4.61. Politics/Opinion;
- 4.2.1.8.4.62. Portal Sites;
- 4.2.1.8.4.63. Potential Criminal Activities;
- 4.2.1.8.4.64. Potential Illegal Software;
- 4.2.1.8.4.65. Potentially Unwanted Programs;
- 4.2.1.8.4.66. Profanity;
- 4.2.1.8.4.67. Professional Networking;
- 4.2.1.8.4.68. Provocative Attire;
- 4.2.1.8.4.69. Public Information;
- 4.2.1.8.4.70. Real Estate;
- 4.2.1.8.4.71. Recreation/Hobbies;
- 4.2.1.8.4.72. Religion/Ideology;
- 4.2.1.8.4.73. Remote Access;
- 4.2.1.8.4.74. Residential IP Addresses
- 4.2.1.8.4.75. Resource Sharing;
- 4.2.1.8.4.76. Restaurants;
- 4.2.1.8.4.77. School Cheating Information;
- 4.2.1.8.4.78. Search Engines;
- 4.2.1.8.4.79. Sexual Materials;
- 4.2.1.8.4.80. Shareware/Freeware;
- 4.2.1.8.4.81. Social Networking;
- 4.2.1.8.4.82. Software/Hardware;
- 4.2.1.8.4.83. Spam URLs;
- 4.2.1.8.4.84. Sports;
- 4.2.1.8.4.85. Stock Trading;
- 4.2.1.8.4.86. Streaming Media;
- 4.2.1.8.4.87. Technical Information;
- 4.2.1.8.4.88. Technical/Business Forums;
- 4.2.1.8.4.89. Text Translators;
- 4.2.1.8.4.90. Text/Spoken Only;
- 4.2.1.8.4.91. Tobacco;
- 4.2.1.8.4.92. Travel;



prodam

CO-05.06/2021

- 4.2.1.8.4.93. Uncategorized;
- 4.2.1.8.4.94. Usenet News;
- 4.2.1.8.4.95. Violence;
- 4.2.1.8.4.96. Visual Search Engine;
- 4.2.1.8.4.97. Weapons;
- 4.2.1.8.4.98. Web Ads;
- 4.2.1.8.4.99. Web Mail;
- 4.2.1.8.4.100. Web Meetings;
- 4.2.1.8.4.101. Web Phone;
- 4.2.1.8.5. Deve ser possível bloquear um site conforme a sua classificação:
 - 4.2.1.8.5.1. Vermelho: Alto Risco;
 - 4.2.1.8.5.2. Amarelo: Médio Risco;
 - 4.2.1.8.5.3. Cinza: Não categorizado;
- 4.2.1.8.6. Deve ser possível bloquear um site quando este nunca foi visto pelo Centro de Inteligência do Fabricante;
- 4.2.1.8.7. Deve ser possível bloquear páginas de phishing, mesmo que o conteúdo tenha acesso permitido;
- 4.2.1.8.8. Deve permitir a varredura de arquivos baixados da internet;
- 4.2.1.8.9. Deve ser possível excluir endereços IP da análise;
- 4.2.1.8.10. Deve permitir a busca segura para buscadores, dentre eles:
 - 4.2.1.8.10.1. Google;
 - 4.2.1.8.10.2. Yahoo;
 - 4.2.1.8.10.3. Bing;
 - 4.2.1.8.10.4. Ask;
- 4.2.1.8.11. Deve bloquear links que direcionem para sites com alto risco;
- 4.2.1.8.12. Deve permitir a customização das mensagens apresentadas para o usuário;
- 4.2.1.8.13. Caso o módulo detecte que exista um McAfee Web Gateway na rede, deverá deixar a análise a cargo deste último;

4.2.1.9. McAfee Device Control

- 4.2.1.9.1. A solução deve ser instalada em computadores com Sistemas Operacionais Windows e OS X/macOS;
- 4.2.1.9.2. A solução deverá permitir o bloqueio total do dispositivo ou apenas o monitoramento;
- 4.2.1.9.3. Deve permitir o controle dos seguintes dispositivos:
 - 4.2.1.9.3.1. Dispositivos de Armazenamento Removíveis;
 - 4.2.1.9.3.2. Dispositivos Bluetooth;
 - 4.2.1.9.3.3. MP3 Players;
 - 4.2.1.9.3.4. Dispositivos Plug and Play;



prodam

CO-05.06/2021

- 4.2.1.9.4. Deve controlar quais dados podem ser copiados para mídias removíveis;
- 4.2.1.9.5. Deve permitir o bloqueio da execução de aplicativos a partir de dispositivos removíveis, podendo criar exceções ao bloqueio;
- 4.2.1.9.6. Deve permitir a proteção de drives USB, smartphones e dispositivos Bluetooth;
- 4.2.1.9.7. Deve controlar o uso de dispositivos por parte dos usuários, como por exemplo:
 - 4.2.1.9.7.1. Mídias Removíveis;
 - 4.2.1.9.7.2. Unidades USB;
 - 4.2.1.9.7.3. Ipods;
 - 4.2.1.9.7.4. Dispositivos Bluetooth;
 - 4.2.1.9.7.5. DVDs;
 - 4.2.1.9.7.6. CDS regraváveis;
- 4.2.1.9.8. A solução deve permitir a proteção de dispositivos móveis com base em:
 - 4.2.1.9.8.1. Classe do Dispositivo:
 - 4.2.1.9.8.1.1. Agrupamento de dispositivos com as mesmas características e possibilidade de gerenciamento do mesmo;
 - 4.2.1.9.8.2. Definição do Dispositivo:
 - 4.2.1.9.8.2.1. Identifica e agrupa dispositivos conforme propriedades comuns;
 - 4.2.1.9.8.3. Regras:
 - 4.2.1.9.8.3.1. Controlam o comportamento do dispositivo;
 - 4.2.1.9.8.4. Deve permitir a configuração dos dispositivos nos modos:
 - 4.2.1.9.8.4.1. Bloqueio, ou;
 - 4.2.1.9.8.4.2. Somente Leitura;
- 4.2.1.9.9. Para a família Windows, deve permitir a classificação dos dispositivos em 3 categorias:
 - 4.2.1.9.9.1. Gerenciado;
 - 4.2.1.9.9.2. Não gerenciado;
 - 4.2.1.9.9.3. Em Lista Branca;
- 4.2.1.9.10. Deve permitir o agrupamento de dispositivos por meio de propriedades comuns, como por exemplo:
 - 4.2.1.9.10.1. VendorID;
 - 4.2.1.9.10.2. ProductID;
 - 4.2.1.9.10.3. Device Class;
- 4.2.1.9.11. Deve ser capaz de identificar o dispositivo (plug and play) através das seguintes informações:
 - 4.2.1.9.11.1. Tipo de USB;
 - 4.2.1.9.11.2. Classe do Dispositivo (Device Class);
 - 4.2.1.9.11.3. ID do fabricante (Vendor ID);



prodam

CO-05.06/2021

- 4.2.1.9.11.4. ID do produto (Product ID);
- 4.2.1.9.12. Deve ser capaz de identificar Dispositivos Removíveis através das seguintes informações:
 - 4.2.1.9.12.1. Tipo de USB;
 - 4.2.1.9.12.2. Se o sistema de arquivo é passível de escrita;
 - 4.2.1.9.12.3. Se o sistema de arquivo é somente leitura;
 - 4.2.1.9.12.4. Tipo de Sistema de Arquivo;
 - 4.2.1.9.12.5. Nome do Sistema de Arquivo;
 - 4.2.1.9.12.6. Número de Série do Sistema de Arquivo;
- 4.2.1.9.13. Deve ser possível habilitar ou desabilitar uma determinada regra de proteção uma vez que esteja dentro da rede (Exemplo: Quando conectado à rede do órgão libera o uso de pen-drive);
- 4.2.1.9.14. Deve possuir as seguintes classes de dispositivos de maneira nativa:
 - 4.2.1.9.14.1. Bateria;
 - 4.2.1.9.14.2. Biometria;
 - 4.2.1.9.14.3. Bluetooth;
 - 4.2.1.9.14.4. Drives de CD/DVD;
 - 4.2.1.9.14.5. Decoders;
 - 4.2.1.9.14.6. Adaptadores de vídeo;
 - 4.2.1.9.14.7. Disco Fixo;
 - 4.2.1.9.14.8. Controladoras de Disquete;
 - 4.2.1.9.14.9. Drives de Disquete;
 - 4.2.1.9.14.10. GPS;
 - 4.2.1.9.14.11. Infravermelho;
 - 4.2.1.9.14.12. IEEE 1394;
 - 4.2.1.9.14.13. Mouse;
 - 4.2.1.9.14.14. Modem;
 - 4.2.1.9.14.15. Fax;
 - 4.2.1.9.14.16. Adaptadores de Rede;
 - 4.2.1.9.14.17. PCMCIA;
- 4.2.1.9.15. Deve possuir os seguintes modelos:
 - 4.2.1.9.15.1. Dispositivos Apple;
 - 4.2.1.9.15.2. Dispositivos BlueTooth;
 - 4.2.1.9.15.3. Drives CD/DVD;
 - 4.2.1.9.15.4. Dispositivos de armazenamento removível;
 - 4.2.1.9.15.5. Leitor de cartão SD;
 - 4.2.1.9.15.6. Dispositivos Windows Portable;
 - 4.2.1.9.15.7. Dispositivos Plug-n-Play USB;
- 4.2.1.9.16. Deve ser possível criar modelos customizados para, no mínimo:
 - 4.2.1.9.16.1. Disco Fixo;
 - 4.2.1.9.16.2. Dispositivo Plug-n-Play;
 - 4.2.1.9.16.3. Dispositivo de Armazenamento Removível;



prodam

CO-05.06/2021

- 4.2.1.9.17. Deve ser possível criar classe de dispositivos customizados utilizando o GUID (Globally Unique Identifier) do dispositivo;
- 4.2.1.9.18. Ao identificar um novo dispositivo conectado no computador cliente, cujo hardware for desconhecido, a solução deve emitir um alerta no console centralizada indicando uma nova classe de dispositivo encontrada;
- 4.2.1.9.19. Deve permitir atrelar um Usuário ou Todos os usuários a um dispositivo específico por meio do seu GUID;
- 4.2.1.9.20. Deve permitir, no console centralizada, a criação dos seguintes controles:
 - 4.2.1.9.20.1. Regra para controle de Dispositivo Citrix XenApp;
 - 4.2.1.9.20.2. Regra para controle de Disco Rígido Fixo;
 - 4.2.1.9.20.3. Regra para dispositivos Plug-n-Play;
 - 4.2.1.9.20.4. Regra para dispositivos de armazenamento removível;
 - 4.2.1.9.20.5. Regra de acesso de arquivos a dispositivos de armazenamento removível;
 - 4.2.1.9.20.6. Regra de Dispositivo TrueCrypt;
 - 4.2.1.9.20.7. Para cada regra, deve ser possível aplicar para:
 - 4.2.1.9.20.7.1. Qualquer usuário (All);
 - 4.2.1.9.20.7.2. Pertencer a um determinado grupo;
 - 4.2.1.9.20.7.3. Pertencer a todos os grupos;
 - 4.2.1.9.20.7.4. Usuário local ou usuário não-LDAP;
 - 4.2.1.9.20.8. Durante a definição da regra, deve permitir a escolha da identificação do objeto LDAP, para, no mínimo:
 - 4.2.1.9.20.8.1. SID do Objeto;
 - 4.2.1.9.20.8.2. Nome do Objeto;
 - 4.2.1.9.20.8.3. Domínio\Nome do Objeto;
 - 4.2.1.9.20.9. Para cada regra deve ser possível configurar exclusões para, no mínimo:
 - 4.2.1.9.20.9.1. Usuários;
 - 4.2.1.9.20.9.2. Dispositivos;
 - 4.2.1.9.20.10. Para cada regra deve ser possível configurar a severidade entre, no mínimo:
 - 4.2.1.9.20.10.1. Informação;
 - 4.2.1.9.20.10.2. Atenção;
 - 4.2.1.9.20.10.3. Menor;
 - 4.2.1.9.20.10.4. Maior;
 - 4.2.1.9.20.10.5. Crítico;
 - 4.2.1.9.20.11. Para cada regra, a solução deve permitir a configuração de reações distintas entre:
 - 4.2.1.9.20.11.1. Computador conectado à rede corporativa;



prodam

CO-05.06/2021

- 4.2.1.9.20.11.2. Computador desconectado da rede corporativa;
- 4.2.1.9.21. Deve possuir capacidade de controlar (Bloquear) o acesso a determinadas extensões ou arquivos TrueType a dispositivos de armazenamento removíveis;
- 4.2.1.9.22. A solução deve permitir que se desabilite uma regra dentre o conjunto de regras.
- 4.2.1.10. McAfee Application Control**
 - 4.2.1.10.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas;
 - 4.2.1.10.2. Deve ser capaz de realizar um inventário nas estações de trabalho protegidas informando todos os executáveis e arquivos de script presentes;
 - 4.2.1.10.3. Como resultado do inventário, a solução deve armazenar:
 - 4.2.1.10.3.1. o nome completo do arquivo;
 - 4.2.1.10.3.2. tamanho;
 - 4.2.1.10.3.3. checksum;
 - 4.2.1.10.3.4. tipo de arquivo;
 - 4.2.1.10.3.5. nome da aplicação e versão;
 - 4.2.1.10.3.6. Ao detectar um executável, a solução deverá consultar o Centro de Inteligência do fabricante que deverá informar um nível de confiança (Bom, Mau ou Não Classificado);
 - 4.2.1.10.4. Deve ser possível criar uma imagem base para a criação de uma política geral;
 - 4.2.1.10.5. Capacidade de trabalhar no modo adaptativo, ou seja, criando regras automaticamente assim que novas aplicações instaladas ou executadas na máquina;
 - 4.2.1.10.6. A solução deverá permitir a realização de varreduras sob demanda em máquinas para executar a blindagem de aplicativos;
 - 4.2.1.10.7. Para o controle de aplicativos, deve possuir, no mínimo, os seguintes modos de operação:
 - 4.2.1.10.7.1. Desabilitado:
 - 4.2.1.10.7.1.1. Proteção desativada;
 - 4.2.1.10.7.2. Monitoramento:
 - 4.2.1.10.7.2.1. Monitora toda a atividade da Estação de Trabalho;
 - 4.2.1.10.7.3. Atualização:
 - 4.2.1.10.7.3.1. A cada execução de aplicativo este é inserido em uma regra ou pacote de autorizações pré-estabelecido;



prodam

CO-05.06/2021

- 4.2.1.10.8. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA-1);
- 4.2.1.10.9. A solução deve suportar as seguintes modalidades de proteção:
 - 4.2.1.10.9.1. Application Whitelisting:
 - 4.2.1.10.9.1.1. Criação de uma lista de aplicações autorizadas que podem ser executadas no equipamento, onde todas as demais aplicações são impedidas de serem executadas;
 - 4.2.1.10.9.2. Application Blocking / Blacklisting:
 - 4.2.1.10.9.2.1. Criação de uma lista de aplicações não autorizadas que não podem ser executadas;
 - 4.2.1.10.9.3. Memory Protection:
 - 4.2.1.10.9.3.1. Monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória;
- 4.2.1.10.10. Solução suporta criação, configuração e manutenção de Whitelist dinamicamente através de definição de regras de confiança;
- 4.2.1.10.11. Em caso de um bloqueio indevido, o usuário poderá submeter o arquivo para revisão do administrador e solicitar a liberação;
- 4.2.1.10.12. Suporta os mecanismos de proteção:
 - 4.2.1.10.12.1. Application Code Protection:
 - 4.2.1.10.12.1.1. Permite que somente os programas em Whitelist (executáveis, binários, DLLs, Scripts, extensões customizadas, etc.) possam ser executados. Além disso, permite proteção contra adulterações de programas em Whitelist (ex.: arquivos do programa) e, opcionalmente, chaves de registros contra modificações em disco;
 - 4.2.1.10.12.2. Memory Protection:
 - 4.2.1.10.12.2.1. Permite proteção contra ataques e exploração de vulnerabilidades para os programas em Whitelist;
- 4.2.1.10.13. Suporta criação, configuração e manutenção de políticas, permitindo ou bloqueando a adesão de Whitelist, através de:



prodam

CO-05.06/2021

- 4.2.1.10.13.1. Binário:
 - 4.2.1.10.13.1.1. Binário específico identificado através de seu nome ou de algoritmo de verificação SHA-1;
- 4.2.1.10.13.2. Trusted Publisher:
 - 4.2.1.10.13.2.1. Fornecedor específico, assinado digitalmente por um certificado de segurança emitido, para este fornecedor, por uma Autoridade Certificadora (CA - Certificate Authority);
- 4.2.1.10.13.3. Trusted Installer:
 - 4.2.1.10.13.3.1. Software instalado por um programa instalador específico, identificações por seu algoritmo de verificação, independentemente de sua origem;
- 4.2.1.10.13.4. Trusted Directories:
 - 4.2.1.10.13.4.1. Pasta compartilhada na rede, onde os programas instaladores para aplicações autorizadas e licenciadas são mantidos;
- 4.2.1.10.13.5. Trusted Program / Authorized Updater:
 - 4.2.1.10.13.5.1. Programas identificados pelo nome, para adicionar e/ou atualizar aplicações;
- 4.2.1.10.13.6. Trusted Users / Authorized Users:
 - 4.2.1.10.13.6.1. Somente usuários selecionados, substituindo a proteção de adulteração, para adicionar e/ou atualizar aplicações.
- 4.2.1.10.13.7. Trusted Time Window / Update Mode:
 - 4.2.1.10.13.7.1. Janela de tempo para manutenção de aplicações;
- 4.2.1.10.14. Deve suportar o uso de variáveis de ambiente para a criação de regras de monitoramento por exemplo:
 - 4.2.1.10.14.1. %HOMEPATH%;
 - 4.2.1.10.14.2. %HOMEDRIVE%;
 - 4.2.1.10.14.3. %USERPROFILE%;
 - 4.2.1.10.14.4. %APPDATA%;
- 4.2.1.10.15. Deve suportar variáveis de ambiente em sistemas 64-bits por exemplo:
 - 4.2.1.10.15.1. %PROGRAMFILES%;
- 4.2.1.10.16. Deve ser possível comparar dois arquivos ou duas versões de um arquivo da mesma estação de trabalho ou de estações diferentes, como forma de mitigar possíveis ameaças persistentes;



prodam

CO-05.06/2021

- 4.2.1.10.17. Deve prover, no mínimo, as seguintes técnicas para proteção de memória de forma a prevenir ataques dia zero:
 - 4.2.1.10.17.1. Critical Address Space Protection;
 - 4.2.1.10.17.2. NX - No eXecute (mp-nx);
 - 4.2.1.10.17.3. Virtual Address Space Randomization;
 - 4.2.1.10.17.4. Mp-vasr-rebase;
 - 4.2.1.10.17.5. Mp-vasr-randomization;
 - 4.2.1.10.17.6. Mp-vasr-relocation;
 - 4.2.1.10.17.7. Mp-vasr-reloc;
 - 4.2.1.10.17.8. Forced DLL Relocation;
- 4.2.1.10.18. Deve possibilitar o controle e bloqueio da instalação de Active-X nas estações de trabalho;
- 4.2.1.10.19. Permitir o bloqueio de aplicações e os processos que a aplicação interage;
- 4.2.1.10.20. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;
- 4.2.1.10.21. Permitir monitoração de Hooking de aplicações onde se podem determinar quais processos podem ser executados;

4.3. ATP – McAfee Adaptive Theat Protection

- 4.3.1.1. McAfee Dynamic Application Containment;
- 4.3.1.2. A solução deve permitir o confinamento dinâmico de aplicativos e arquivos executáveis com característica maliciosa (Exemplo: Ransomware);
- 4.3.1.3. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas executando-as em ambiente controlado;
- 4.3.1.4. Deve permitir a indicação de aplicações confiáveis para que não caiam no filtro de confinamento dinâmico;
- 4.3.1.5. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;
- 4.3.1.6. Solução deve manter um cache de reputação local com informações de aplicações – conhecidas, desconhecidas e maliciosas;
- 4.3.1.7. Deve ser possível a classificação de cada aplicativo de maneira manual e até mesmo sua reclassificação através da console de administração central;
- 4.3.1.8. Dentre os comportamentos maliciosos, deve ser capaz de:
 - 4.3.1.8.1. Bloquear acesso local a partir de cookies;
 - 4.3.1.8.2. Criação de arquivos a partir de arquivos com extensão:
 - 4.3.1.8.2.1. .bat;
 - 4.3.1.8.2.2. .exe;
 - 4.3.1.8.2.3. .html;



prodam

CO-05.06/2021

- 4.3.1.8.2.4. .hpg;
- 4.3.1.8.2.5. .bmp;
- 4.3.1.8.2.6. .job;
- 4.3.1.8.2.7. .vbs
- 4.3.1.8.3. Criação de arquivos em qualquer local de rede;
- 4.3.1.8.4. Criação de novos CLSIDs, APPIDs e TYPELIBs;
- 4.3.1.8.5. Criação de threads em outro processo;
- 4.3.1.8.6. Bloquear a desativação de executáveis críticos do sistema operacional;
- 4.3.1.8.7. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;
- 4.3.1.8.8. Gravação e Leitura na memória de outro processo;
- 4.3.1.8.9. Bloqueio de Modificação da política de firewall do Windows;
- 4.3.1.8.10. Bloqueio de Modificação da pasta de tarefas do Windows;
- 4.3.1.8.11. Bloqueio de Modificação de arquivos críticos do Windows e Locais do Registro;
- 4.3.1.8.12. Bloqueio de Modificação de arquivos executáveis portáteis;
- 4.3.1.8.13. Bloqueio de Modificação de bit de atributo oculto
Bloqueio de Modificação de bit de atributo somente leitura;
- 4.3.1.8.14. Bloqueio de Modificação de entradas de registro de DLL Applnit;
- 4.3.1.8.15. Bloqueio de Modificação de locais do registro de inicialização;
- 4.3.1.8.16. Bloqueio de Modificação de pastas de dados de usuários;
- 4.3.1.8.17. Bloqueio de Modificação do local do Registro de Serviços;
- 4.3.1.8.18. Bloqueio de Suspensão de um processo;
- 4.3.1.8.19. Bloqueio de Término de outro processo;
- 4.3.1.8.20. Dos comportamentos observados, deve ser possível bloquear ou apenas informar caso o mesmo ocorra;
- 4.3.1.8.21. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem customizada;
- 4.3.1.8.22. O modo de ativação do confinamento dinâmico para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca visto pela solução;
- 4.3.1.8.23. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;



prodam

CO-05.06/2021

4.3.1.8.24. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção;

4.3.1.9. McAfee Real Protect:

4.3.1.9.1. Deve permitir que o mecanismo trabalhe apenas em modo de observação;

4.3.1.9.2. Deve permitir a análise de processos iniciados em drives mapeados de rede;

4.3.1.9.3. Deve ser capaz de trabalhar com técnicas de análise matemática para identificação de ameaças sem a necessidade de assinaturas;

4.3.1.9.3.1. Deve permitir a operação:

4.3.1.9.3.2. Apenas no cliente;

4.3.1.9.3.3. No cliente e integrada com a Nuvem do fabricante;

4.3.1.9.3.4. Ao selecionar a análise apenas no cliente, deve ser possível indicar a sensibilidade do motor de análise;

4.3.1.9.4. Deve permitir a seleção do melhor modo de operação da solução, variando entre:

4.3.1.9.4.1. Modo Balanceado;

4.3.1.9.4.2. Modo Produtividade;

4.3.1.9.4.3. Modo Segurança;

4.3.1.9.5. Deve ativar o módulo de confinamento dinâmico, de maneira automática, caso uma ameaça atinja um determinado nível de criticidade a ser indicado pelo administrador da solução;

4.4. TIE - McAfee Threat Intelligence Exchange

4.4.1. O módulo de reputação local deve manter uma base de dados com todos os executáveis detectados no ambiente;

4.4.2. Para cada executável, deverão ser apresentadas as reputações:

4.4.2.1. Local;

4.4.2.2. Centro de Inteligência do Fabricante;

4.4.2.3. Analisador Dia Zero;

4.4.2.4. Filtro de Conteúdo Web;

4.4.3. Deve permitir uma visualização analítica sobre cada arquivo detectado no ambiente, com no mínimo as seguintes informações:

4.4.3.1. Data do último acesso;

4.4.3.2. Tamanho do arquivo;

4.4.3.3. Se está listado no Adicionar/Remover programas do Windows;

4.4.3.4. Data de compilação;

4.4.3.5. Registrado como serviço;



prodam

CO-05.06/2021

- 4.4.3.6. Registrado para executar automaticamente;
- 4.4.3.7. Mais de 6 meses de idade;
- 4.4.3.8. Idade foi falsificada;
- 4.4.3.9. Executado a partir do cmd.exe;
- 4.4.4. Deve ser capaz de informar a URL de origem do arquivo e sua reputação;
- 4.4.5. Deve permitir integração com base global de vírus – VirusTotal – para comparação e se o arquivo sob análise já foi detectado por outro fabricante de segurança, permitindo que esta informação seja utilizada para a indicação de que o artefato é malicioso ou não;
- 4.4.6. Deve permitir o rastreamento da execução do arquivo malicioso pelo ambiente informando qual foi a sua primeira execução e sua última;
- 4.4.7. Deve permitir a identificação da estação de trabalho e do usuário associado a mesma;
- 4.4.8. O módulo deve permitir automatização de contramedidas a partir de soluções do mesmo fabricante e de fabricantes terceiros;

5. ATD – McAfee Virtual Advanced Threat Defense Appliance

5.1. Quantidades: 37.800

- 5.1.1. **8 instâncias de SandBox em cada servidor**
- 5.1.2. Aquisição de novas Licenças da Suíte McAfee Virtual Advanced Threat Defense Appliance:
 - 5.1.2.1. 3 (três) servidores. McAfee Advanced Threat Defence Software, cada servidor teremos 8 instâncias de SandBox;
- 5.1.3. **Características dos 3 Servidores**
 - 5.1.3.1. A solução deve suportar implementação em hardware virtual dos hypervisors VMWare e Hiper-V.
 - 5.1.3.2. Deve ser fornecido no mínimo 3 servidores para virtualização, que será de responsabilidade da CONTRATADA os fornecimentos dos seus respectivos recursos de hardwares e softwares mínimos para o funcionamento do produto;
- 5.1.4. **Características Gerais da Solução**
 - 5.1.4.1. O conjunto deverá operar em modo out-of-band (passivo) não introduzindo latência na banda diretamente;
 - 5.1.4.2. O conjunto proposto deverá ser capaz de inspecionar os seguintes tipos de tráfego de rede:
 - 5.1.4.2.1. HTTP e HTTPS, recebidos através de servidor de proxy;
 - 5.1.4.2.2. SMTP, recebido através de gateway SMTP;
 - 5.1.4.3. Os arquivos deverão ser submetidos por meio de:
 - 5.1.4.3.1. Upload Manual;
 - 5.1.4.3.2. REST API;
 - 5.1.4.3.3. FTP;
 - 5.1.4.4. Integração Nativa via:
 - 5.1.4.4.1. McAfee Web Gateway;
 - 5.1.4.4.2. McAfee Email Gateway e McAfee ePolicy Orchestrator;
 - 5.1.4.4.3. McAfee Threat Intelligence Exchange;



prodam

CO-05.06/2021

- 5.1.4.4.4. Bro Network Sensor;
- 5.1.4.4.5. McAfee Application Control;
- 5.1.4.4.6. McAfee Move Multiplatform;
- 5.1.4.5. Não serão aceitos equipamentos que se encontrem na situação de end-of-support, com previsão de descontinuidade de suporte pelo fabricante;
- 5.1.4.6. As licenças de uso de software serão adquiridas em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante ou seu representante;
- 5.1.4.7. Não serão aceitos equipamentos e softwares personalizados para que sejam diferentes dos oferecidos pelo fabricante para o mercado em geral;
- 5.1.4.8. Os equipamentos entregues deverão ser novos, de primeiro uso, entregue em perfeito estado de funcionamento;
 - 5.1.4.8.1. A Prodam fará a checagem da conformidade em até 10 dias corridos após a entrega dos equipamentos em sua unidade.
 - 5.1.4.8.2. Caso haja irregularidades a CONTRATADA deverá substituir os equipamentos em até 15 dias corridos, sendo descontados do prazo final de entrega dos equipamentos (60 dias), se existir. Neste caso aplicado multa sobre atraso da entrega, conforme item 16.5
- 5.1.4.9. Possuir recursos de operação em alta disponibilidade (cluster), suportando tecnologias de redundância e balanceamento de carga;
- 5.1.4.10. Deverá suportar no mínimo, 16 (dezesseis) nós no cluster;
- 5.1.4.11. O Cluster não deverá ter restrição de implementação em um único tipo de equipamento em hardware e deve permitir a mescla de modelos de hardware distintos;
- 5.1.4.12. Interface de administração via navegadores web ou software client;
- 5.1.4.13. Interface em Linha de Comando (CLI) com acesso via SSH que forneça funções de administração e monitoramento dos equipamentos;
- 5.1.4.14. Acesso à GUI por meio de protocolos seguros, como o HTTPS;
- 5.1.4.15. Apresentar painel de status (dashboard) do equipamento, incluindo informações sobre alertas ativos, proteções aplicadas ao tráfego, total de objetos analisados bloqueados e/ou alertados;



prodam

CO-05.06/2021

- 5.1.4.16. Exibição de processos em execução em ambiente virtualizado automatizado, download em formato binário do Malware e/ou código malicioso e apresentação análise comportamental incluindo listagem de módulos e processos utilizados pelo Malware e/ou código malicioso de forma sequencial;
- 5.1.4.17. A GUI do equipamento deve exibir arquivos de log contendo o registro de todos os eventos relevantes que possam afetar a sua administração, incluindo login de usuários, as alterações de configuração, comandos efetuados pela interface de linha de comando (CLI) e eventos administrativos automatizados, como atualizações das definições de assinaturas e aplicações de novas firmwares;

5.1.5. **Características do Performance**

- 5.1.5.1. O equipamento deverá ser capaz de efetuar a seguinte carga de análise:
 - 5.1.5.1.1. No mínimo, 4.000 (quatro mil) objetos por dia;
 - 5.1.5.1.2. O equipamento deverá ser capaz de suportar a seguinte quantidade de instâncias de máquinas virtuais em execução simultânea para análise dinâmica de arquivos:
 - 5.1.5.1.3. No mínimo, 8 (oito) instâncias de máquinas virtuais;
 - 5.1.5.1.4. A solução ofertada deverá atender todo o ambiente protegido pelos antivírus de desktops/servidores descritos neste documento.

5.1.6. **Características de Segurança e Análise de Arquivos**

- 5.1.6.1. Deve ser capaz de analisar os seguintes tipos de arquivos em análise dinâmica e estática:
 - 5.1.6.1.1. Arquivos Executáveis (.exe, .dll, .scr, .ocx, .sys, .com, .drv, .cpl, .cgi);
 - 5.1.6.1.2. Arquivos Office (.doc, .dotm, .docx, .dotx, .xls, .ppam, .xlsx, .pps, .xlsb, .ppsx, .xlsm, .ppsm, .ppt, .ppt, .pptx, .pptm, .rtf, .shs, .xltm, .sldm, .xltx, .sldx, .xlam, .thmx, .docm, .xar);
 - 5.1.6.1.3. Arquivos Compactados (.gz, .msi, .tgz, .lzh, .zip, .lzma, .cab, .iso, .7z);
 - 5.1.6.1.4. Adobe (.pdf, .swf);
 - 5.1.6.1.5. Arquivos de Aplicativos Android (.apk);
 - 5.1.6.1.6. Arquivos Java (.jar, .class, .js, arquivos Java bin);
 - 5.1.6.1.7. Arquivos de execução em lote e outros tipos de arquivo (.cmd, .ace, .bat, .arj, .vbs, .chm, .xml, .lnk, .url, .mof, .htm, .ocx, .html, .potm, .eml, .potx, .mht, .ps1, .msg, .reg, .vb, .wsc, .vba, .wsf, .vbe, .wsh, .vbs);



CO-05.06/2021

- 5.1.6.2. Deve ser capaz de analisar os seguintes tipos de arquivos, ao menos, em análise estática:
 - 5.1.6.2.1. Arquivos de imagem (.jpeg, .png, .gif);
- 5.1.6.3. Dispor de mecanismos distintos para verificação de arquivos e artefatos maliciosos, contendo, no mínimo:
 - 5.1.6.3.1. Integração com o centro de inteligência do fabricante para verificar a reputação da arquivos e de URLs acessadas pelo arquivo;
 - 5.1.6.3.2. Listas negras ou brancas para condenação ou liberação de arquivos;
 - 5.1.6.3.3. Permitir o suporte a customização de regras no padrão YARA para identificação de diretórios ou arquivos suspeitos;
- 5.1.6.4. Emulação da execução de arquivos em máquinas virtuais executadas sob demanda com coleta de características e comportamento da amostra quando executada;
- 5.1.6.5. No mínimo, 2 (dois) mecanismos de varredura de vírus distintos (antivírus engine);
- 5.1.6.6. Componente que desempacote arquivos (unpacking);
- 5.1.6.7. Componente que faça análise estática de código;
- 5.1.6.8. Componente que faça a desmontagem (Disassembly) do código;
- 5.1.6.9. Componente que utilize redes neurais estatísticas baseadas em aprendizado de máquina (Machine Learning);
- 5.1.6.10. Deve realizar análise heurística (IE-FFx-Acrobat Emulation) baseado em análise estatística comportamental da geometria do arquivo, semântica e comportamento do código;
- 5.1.6.11. Deve permitir o uso de Deep Neural Network Prediction para a detecção de ameaças;
- 5.1.6.12. Deve realizar a análise estática de código e aplicar a engenharia reversa automatizada e o disassembly da análise de código;
- 5.1.6.13. Deve permitir a análise de modo interativo durante a execução dinâmica do código;
- 5.1.6.14. Deve permitir que as máquinas virtuais utilizadas para análise dinâmica (sandboxing) sejam personalizadas, permitindo escolha de sistema operacional, instalação de programas, customizações de usuário e de outros aspectos do sistema operacional;
- 5.1.6.15. Deve permitir a criação de perfis de análises contendo, no mínimo, 3 (três) tipos de máquinas virtuais com sistemas operacionais distintos para utilização em análise dinâmica (sandboxing), bem como ativar ou desativar mecanismos de verificação de forma selecionada;
- 5.1.6.16. A análise dinâmica deve suportar a execução nos seguintes sistemas operacionais como máquinas virtual de análise:
 - 5.1.6.16.1. Android;
 - 5.1.6.16.2. Microsoft Windows 7 32-bit (Service Pack 1);



prodam

CO-05.06/2021

- 5.1.6.16.3. Microsoft Windows 7 64-bit (Service Pack 1);
 - 5.1.6.16.4. Microsoft Windows 8 Professional 32-bit;
 - 5.1.6.16.5. Microsoft Windows 8 Professional 64-bit;
 - 5.1.6.16.6. Microsoft Windows 8.1 64-bit Enterprise (Update 1 version 6.3 build 9600);
 - 5.1.6.16.7. Microsoft Windows 8.1 64-bit Professional (Update 1 version 6.3 build 9600);
 - 5.1.6.16.8. Microsoft Windows 10 Professional (version 1607);
 - 5.1.6.16.9. Microsoft Windows 10 Enterprise 64-bit (Redstone 1 and 2, Threshold 2);
 - 5.1.6.16.10. Microsoft Windows Server 2008 R2 (Service Pack 1);
 - 5.1.6.16.11. Microsoft Windows Server 2012 Standard;
 - 5.1.6.16.12. Microsoft Windows Server 2012 R2 Standard
 - 5.1.6.16.13. Microsoft Windows Server 2012 Datacenter;
 - 5.1.6.16.14. Microsoft Windows Server 2012 R2 Datacenter;
 - 5.1.6.16.15. Microsoft Windows Server 2016 Standard;
 - 5.1.6.17. Deve suportar a submissão de URLs para análise;
 - 5.1.6.18. Deve ser capaz de inspecionar arquivos criptografados;
 - 5.1.6.19. Toda a verificação e análise de Malwares e/ou códigos maliciosos devem ocorrer em tempo real, não sendo aceitas verificações em segundo plano;
 - 5.1.6.20. Analisar de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;
 - 5.1.6.21. Deve possuir mecanismo para a identificação de Malwares em anexos de e-mails e URLs;
 - 5.1.6.22. Detectar Malwares que utilizem mecanismo de Exploit em arquivos, como PDF;
- 5.1.7. **Características de Relatórios**
- 5.1.7.1. A análise forense apresentada no relatório deve incluir:
 - 5.1.7.1.1. Um gráfico detalhado dos componentes e a lógica dos caminhos de execução;
 - 5.1.7.1.2. Endereços IP com o qual a amostra interagiu;
 - 5.1.7.1.3. Reputação de URLs acessadas;
 - 5.1.7.1.4. Interações com arquivos acessados pela amostra;
 - 5.1.7.1.5. Interações com entradas e chaves de registro feitas pela amostra;
 - 5.1.7.1.6. Operações realizadas em arquivos;
 - 5.1.7.1.7. Diretórios e arquivos criados;
 - 5.1.7.1.8. Arquivos que possam ter sido baixados pela amostra;
 - 5.1.7.1.9. Características apresentadas pelo arquivo em classificação de comportamentos:
 - 5.1.7.1.10. Persistência;
 - 5.1.7.1.11. Comunicação em rede;



prodam

CO-05.06/2021

- 5.1.7.1.12. Evasão de soluções de segurança e execução em ambiente controlado;
- 5.1.7.1.13. Capacidade de multiplicação em ambiente de rede;
- 5.1.7.1.14. Proteção contra remoção e camuflagem;
- 5.1.7.1.15. Características de espionagem, captura de tráfego, captura de dados digitados;
- 5.1.7.2. Engine que condenou a amostra ou engines que analisaram a amostra;
- 5.1.7.3. O relatório de forense deve prover uma porcentagem geral de parte do código contra a porcentagem da execução durante a análise dinâmica;
- 5.1.7.4. O relatório forense deve indicar o re-uso de segmentos de código de malwares e prover a classificação da família ao qual o malware se enquadra;
- 5.1.7.5. O relatório deve estar disponível nos formatos HTML, PDF, texto;
- 5.1.7.6. Deve permitir a exportação de informação por meio de STIX, OpenIOC para sistemas terceiros (Exemplo: SIEM).

5.1.8. Características de Integrações

- 5.1.8.1. Através da integração com o ePolicy Orchestrator, a solução deve buscar informações relacionadas ao sistema afetado, como por exemplo, sistema operacional. Este tipo de informação deverá ser utilizado para nortear a análise dinâmica, ou seja, escolher uma máquina virtual similar;
- 5.1.8.2. Após detectar uma ameaça com severidades média, alta ou muito alta, o arquivo deve ser inserido em uma blacklist de forma a não permitir que usuários façam downloads;

6. McAfee Move AV for Virtual Server

6.1. Quantidade: 800 licenças

- 6.1.1. A solução de antivírus deverá ser dedicada a plataforma de servidores virtualizados utilizando no mínimo a tecnologia VMWare. A solução deve oferecer proteção e segurança antimalware sem prejudicar o desempenho. A solução de Antivírus deve no mínimo assegurar:
 - 6.1.1.1. **Otimização da segurança de ambientes virtualizados:** a solução de Antivírus para servidores virtualizados deverá minimizar o impacto sobre o desempenho em servidores virtuais com um mecanismo aprimorado que se baseia na carga total do hypervisor para realizar varreduras ou evitá-las;



proclam

CO-05.06/2021

- 6.1.1.2. **Padronização da segurança em todos os principais hipervisores:** seja no começo de uma distribuição de máquinas virtuais ou na continuação de um processo adiantado de computação na nuvem, o Antivírus deve oferecer a flexibilidade da segurança consistente em todos os principais hipervisores;
 - 6.1.1.3. **Garantia do gerenciamento de segurança e entrega em ambientes virtualizados:** utilizar e aperfeiçoar a proteção do McAfee VirusScan Enterprise em ambientes virtualizados, proporcionando gerenciamento de segurança e eficácia com o console do McAfee ePolicy Orchestrator (ePO existente, no qual gerencia mais de 37.000 agentes instalados em estações de trabalho da PMSP). Garanta a integridade das políticas de segurança, mesmo durante a migração de máquinas virtuais no ambiente virtualizado;
 - 6.1.1.4. **Redução dos recursos de varredura de vírus em ambientes de servidores e desktops virtuais:** Reduzir os recursos individuais de máquinas virtuais necessários para contemplar o processamento antivírus tradicionais, liberando-os para outras tarefas essenciais;
 - 6.1.1.5. **Flexibilidade na distribuição de segurança de infraestrutura virtual:** Oferecer uma segurança preparada para todo o ambiente virtual com suporte a todos os principais hipervisores;
 - 6.1.1.6. **Maior eficiência operacional para a segurança da infraestrutura virtual:** Garantir que a varredura por vírus não prejudicará o desempenho operacional agendando funções de varredura com base na carga geral do hipervisor para servidores virtuais, e diminua o processamento de varreduras em ambientes de servidores e desktops virtuais;
 - 6.1.1.7. **Simplicidade no gerenciamento da segurança de terminais:** Realizar o gerenciamento e a geração de relatórios de políticas em todos os tipos de ambientes de terminais e servidores por meio do software McAfee ePolicy Orchestrator (ePO), sejam os terminais físicos ou virtuais.
- 6.1.2. **Características mínimas exigidas:**
- 6.1.2.1. **Arquitetura de Solução:**
 - 6.1.2.1.1. A solução deverá dispensar a instalação de agentes de varredura em todas as máquinas virtuais hospedadas em um servidor de virtualização;
 - 6.1.2.1.2. A solução deve implementar o uso de um servidor de varredura Offload, que será responsável por escanear todos os acessos de arquivos nas máquinas virtuais hospedadas em determinado servidor Hypervisor, resultando assim em menos consumo de recursos e melhoria de desempenho;



prodam

CO-05.06/2021

- 6.1.2.1.3. A solução deve prover gerenciamento centralizado, a partir da mesma solução de gerência já utilizada pelos agentes de antivírus convencionais utilizados na rede (ePO - Eletronic ePolicy Orchestrator);
- 6.1.2.1.4. Esse servidor de gerenciamento deve servir também como repositório de políticas e atualizações para o produto de proteção a virtualização;
- 6.1.2.1.5. O servidor de varredura offload deve permitir a implementação em alta disponibilidade, aumentando assim o nível de segurança e deixando o ambiente preparado para o evento de falha do servidor de varredura;
- 6.1.2.1.6. O módulo para proteção de infraestrutura virtual, deverá proporcionar a proteção de ambientes virtualização VMWare e Microsoft Hyper V no mínimo;
- 6.1.2.2. A solução deverá permitir a sua implantação atendendo no mínimo uma das seguintes opções:
 - 6.1.2.2.1. Multiplataforma, atuando para realizar o rastreamento em tempo real, por demanda e agendado de malwares, através da utilização de uma máquina virtual com a solução Antivírus instalada efetuando todas as análises da estrutura, sem a necessidade de qualquer integração com agentes externos ou a instalação de clientes Antivírus em cada uma das máquinas virtuais;
 - 6.1.2.2.2. Sem agente, atuando para realizar o rastreamento de malwares em tempo real, por demanda e agendado, através de integração com o VMWare vShield 5.0 utilizando o VMWare vShield para rastreamento automático em ambientes que contém o SVA (Storage Virtual Appliance);
- 6.1.2.3. Deverá oferecer suporte para instalação do servidor de varredura no mínimo nas seguintes plataformas:
 - 6.1.2.3.1. Windows 2008 R2 SP1;
 - 6.1.2.3.2. Windows 2008 SP2 (64-bit);
 - 6.1.2.3.3. Windows 2012;
 - 6.1.2.3.4. Windows 2012 R2;
 - 6.1.2.3.5. Windows 2016;
 - 6.1.2.3.6. Windows 2019;
- 6.1.2.4. Deverá oferecer suporte para proteção de máquinas virtuais utilizando NO MÍNIMO os seguintes sistemas operacionais:
 - 6.1.2.4.1. Windows 7 SP1 (32 ou 64 bits);
 - 6.1.2.4.2. Windows 8 (32 ou 64 bits);
 - 6.1.2.4.3. Windows 10 (32 ou 64 bits);
 - 6.1.2.4.4. Windows 2008 SP2 (32 ou 64 bits);
 - 6.1.2.4.5. Windows 2008 R2 SP1 (64 bits);



prodam

CO-05.06/2021

- 6.1.2.4.6. Windows 2012 (64 bits);
- 6.1.2.4.7. Windows 2012 R2 (64 bits);
- 6.1.2.4.8. Windows 2016 (64 bits);
- 6.1.2.4.9. Windows 2019 (64 bits);
- 6.1.2.5. Console de Gerência da Solução:
 - 6.1.2.5.1. Deverá oferecer suporte à instalação em um servidor nas plataformas Windows Server 2008 (Com Service Pack 2 ou superior) 32 e 64 bits e Windows 2008 Server R2 e Windows 2008 Small Business Server somente em 64-bit, ou superior;
 - 6.1.2.5.2. O gerenciamento deve permitir operar em alta-disponibilidade;
 - 6.1.2.5.3. O gerenciador deverá prover ao administrador ferramentas que possibilitem o Backup e Restore de políticas;
 - 6.1.2.5.4. A ferramenta de gerência deve possibilitar autenticação externa integrada a estrutura LDAP;
 - 6.1.2.5.5. A ferramenta de gerência deve suportar o gerenciamento de políticas de senha de autenticação no console;
 - 6.1.2.5.6. A solução de gerenciamento deve permitir acesso a sua console via web;
 - 6.1.2.5.7. A ferramenta de gerenciamento deverá permitir a criação de dashboards que permitam identificar em tempo real o nível de atualização do ambiente;
- 6.1.2.6. Permitir a alteração das configurações da Solução nos clientes de maneira remota;
- 6.1.2.7. Permitir a distribuição remota do agente de proteção para as máquinas virtuais;
- 6.1.2.8. Permitir a distribuição remota do software para os servidores que hospedam as máquinas virtuais;
- 6.1.2.9. Permitir o gerenciamento do servidor através do protocolo TCP/IP e HTTP
- 6.1.2.10. A ferramenta de gerência deve suportar a autenticação com segregação de funções, possibilitando a criação de usuários com diferentes níveis de permissão (Relatórios, auditoria, configuração);
- 6.1.2.11. Customização dos relatórios gráficos gerados;
- 6.1.2.12. Exportação dos relatórios para os seguintes formatos os seguintes formatos:
 - 6.1.2.12.1. HTML, CSV, PDF;
 - 6.1.2.12.2. Geração de relatórios que contenham as seguintes informações:
 - 6.1.2.12.3. Os vírus que mais foram detectados;
 - 6.1.2.12.4. As máquinas que mais sofreram infecções em um determinado período;



prodam

CO-05.06/2021

- 6.1.2.12.5. Os usuários que mais sofreram infecções em um determinado período;
- 6.1.2.12.6. Gerenciamento de todos os módulos da suíte;
- 6.1.2.13. Deve possuir log de auditoria, logando todas as ações dos usuários na console de gerenciamento.
- 6.1.2.14. Gerenciamento de políticas e configuração:
 - 6.1.2.14.1. A aplicação deve conter um conjunto de políticas pré-configuradas;
 - 6.1.2.14.2. A solução deverá permitir a realização de varreduras por demandas em máquinas virtuais que estiverem em estado "offline";
 - 6.1.2.14.3. O servidor de varredura offload deve permitir acesso a configuração e verificação de estatísticas via linha de comando CLI (Command Line Interface);
- 6.1.2.15. Deverá permitir a tomada de no mínimo as seguintes ações quando uma ameaça for identificada no servidor e nas máquinas clientes:
 - 6.1.2.15.1. Limpar o arquivo automaticamente;
 - 6.1.2.15.2. Excluir o arquivo automaticamente;
 - 6.1.2.15.3. Negar o acesso ao arquivo;
- 6.1.2.16. Na falha da execução da primeira ação deverá permitir a configuração de ação secundária com no mínimo as seguintes opções:
 - 6.1.2.16.1. Excluir o arquivo automaticamente;
 - 6.1.2.16.2. Negar o acesso ao arquivo;
- 6.1.2.17. Deverá permitir a aplicação de ações diferenciadas para Malwares e programas potencialmente indesejados (PUP's);

7. Suporte Manutenção e Subscrição da Licença do Antivírus MFE VirusScan for Storage NAS

7.1. Quantidade: 01 Licença

7.1.1. Características Mínimas Exigidas:

- 7.1.1.1. Atualização da licença atual e suporte ao NAS EMC² VNX5400 Versão 8.1.9-184 ou superior;
- 7.1.1.2. Permitir análise dos arquivos armazenados no momento de leitura e gravação no NAS e quarentenar imediatamente arquivos suspeitos;
- 7.1.1.3. Deve possuir suporte e integração com o módulo de inteligência contra ameaças, ou seja, ao identificar um determinado arquivo, este deverá ser verificado quanto a sua reputação na base centralizada ou no serviço de nuvem do fabricante;
- 7.1.1.4. Permitir integração com console de gerenciamento centralizado para visualização de relatórios pertinentes as detecções efetuadas nos arquivos armazenados no ambiente NAS;



prodam

CO-05.06/2021

- 7.1.1.5. A solução anti-malware em seu processo de escaneamento não deverá comprometer o desempenho computacional do sistema de armazenamento e gerenciamento de dados (NAS);
- 7.1.1.6. Deverá permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação a solução anti-malware tomará para arquivos infectados;
- 7.1.1.7. Possibilitar notificações de eventos e envio de alertas de forma automática para o administrador;
- 7.1.1.8. A solução anti-malware deverá permitir a configuração de escaneamento nas seguintes modalidades:
 - 7.1.1.8.1. Escaneamento em tempo real;
 - 7.1.1.8.2. Escaneamento agendado.
- 7.1.1.9. A solução anti-malware deverá permitir a configuração de uma lista de tipos de extensões predeterminadas pelo administrador do sistema para os processos de escaneamento;
- 7.1.1.10. A solução em seu processo de escaneamento não deverá comprometer o desempenho computacional do sistema de armazenamento e gerenciamento de dados (NAS);
- 7.1.1.11. Deverá fornecer proteção anti-malware em tempo real para EMC, NetApp, Hitachi e IBM;
- 7.1.1.12. Deverá fornecer suporte CAVA Agent e aos protocolos RPC e ICAP;
- 7.1.1.13. Permitir configurações flexíveis de escaneamento;
- 7.1.1.14. Fornece suporte ao monitoramento de rede via SNMP/MOM;
- 7.1.1.15. Compatibilidade mínima:
 - 7.1.1.15.1. Software:
 - 7.1.1.15.1.1. Microsoft Windows Server 2008/2008 R2 x86/x64 Standard / Enterprise/ Datacenter Edition (incluindo modo Core);
 - 7.1.1.15.1.2. Microsoft Windows Server 2012/2012 R2 Essentials / Standard / Foundation / Datacenter incluindo modo Core);
- 7.1.1.16. Suportar, no mínimo, as Plataformas:
 - 7.1.1.16.1. EMC Celerra / VNX file storages:
 - 7.1.1.16.1.1. EMC DART 6.0.36 ou superior;
 - 7.1.1.16.1.2. Celerra Antivírus Agent (CAVA) 4.5.2.3 ou superior.
 - 7.1.1.16.2. EMC Isilon Storage:
 - 7.1.1.16.2.1. EMC Isilon OneFS 7.0.
 - 7.1.1.16.3. EMC NetApp Storages:
 - 7.1.1.16.3.1. NetApp Data ONTAP 7.x e 8.x em 7 mode;
 - 7.1.1.16.3.2. NetApp Clustered Data ONTAP 8.x e 9.x.
 - 7.1.1.16.4. IBM Storages:
 - 7.1.1.16.4.1. IBM System Storage N Series;
 - 7.1.1.16.5. Hitachi Storages:



prodam

CO-05.06/2021

- 7.1.1.16.5.1. HNAS 4100;
- 7.1.1.16.5.2. HNAS 4080;
- 7.1.1.16.5.3. HNAS 4060;
- 7.1.1.16.5.4. HNAS 4040;
- 7.1.1.16.5.5. HNAS 3090;
- 7.1.1.16.5.6. HNAS 3080.
- 7.1.1.16.6. NAS:
 - 7.1.1.16.6.1. iCap compatível ou PRC Compatível NAS.
- 7.1.1.16.7. DELL:
 - 7.1.1.16.7.1. DELL FS8600 on FluidFS 6.x;
 - 7.1.1.16.7.2. DELL FS8600 on FluidFS 5.x.
- 7.1.2. Características Mínimas:
 - 7.1.2.1. Proteção anti-malware em tempo real para EMC, NetApp, Hitachi e IBM;
 - 7.1.2.2. Suporte CAVA Agent e aos protocolos RPC e ICAP;
 - 7.1.2.3. Permitir configurações flexíveis de escaneamento;
 - 7.1.2.4. Permitir utilização adaptável dos recursos do sistema;
 - 7.1.2.5. Suporte ao monitoramento de rede via SNMP/MOM;
 - 7.1.2.6. Suportar o gerenciamento dos vírus com base de dados de no mínimo 100 Tb armazenados;
 - 7.1.2.7. Permitir integração com console de gerenciamento centralizado para visualização de relatórios pertinentes as detecções efetuadas nos arquivos armazenados no ambiente NAS;
 - 7.1.2.8. Bloquear malware antes que ele faça seu caminho para seus dispositivos NAS;
 - 7.1.2.9. Verificar arquivos em tempo real quando eles são adicionados ou modificados.
 - 7.1.2.10. Permitir análise dos arquivos armazenados no momento de leitura e gravação no NAS;
 - 7.1.2.11. Suporte ao gerenciamento dos vírus com base de dados de no mínimo 100 Tb armazenados;
 - 7.1.2.12. Permitir integração com console de gerenciamento centralizado para visualização de relatórios pertinentes as detecções efetuadas nos arquivos armazenados no ambiente NAS.

8. Suporte e Manutenção para as novas Licenças do Antivírus MFE VirusScan for Storage NAS

8.1. Quantidade: 03 Licenças

- 8.1.1. Características Mínimas Exigidas:
 - 8.1.1.1. Aquisição de novas licenças, suporte e manutenção ao NAS EMC² VNX5400 Versão 8.1.9-184 ou superior;



prodam

CO-05.06/2021

- 8.1.1.2. Permitir análise dos arquivos armazenados no momento de leitura e gravação no NAS e quarentenar imediatamente arquivos suspeitos;
- 8.1.1.3. Deve possuir suporte e integração com o módulo de inteligência contra ameaças, ou seja, ao identificar um determinado arquivo, este deverá ser verificado quanto a sua reputação na base centralizada ou no serviço de nuvem do fabricante;
- 8.1.1.4. Permitir integração com console de gerenciamento centralizado para visualização de relatórios pertinentes as detecções efetuadas nos arquivos armazenados no ambiente NAS;
- 8.1.1.5. A solução anti-malware em seu processo de escaneamento não deverá comprometer o desempenho computacional do sistema de armazenamento e gerenciamento de dados (NAS);
- 8.1.1.6. Deverá permitir configuração de ações para arquivos infectados com console de interface gráfica intuitiva para que o administrador configure qual ação a solução anti-malware tomará para arquivos infectados;
- 8.1.1.7. Possibilitar notificações de eventos e envio de alertas de forma automática para o administrador;
- 8.1.1.8. A solução anti-malware deverá permitir a configuração de escaneamento nas seguintes modalidades:
 - 8.1.1.8.1. Escaneamento em tempo real;
 - 8.1.1.8.2. Escaneamento agendado.
- 8.1.1.9. A solução anti-malware deverá permitir a configuração de uma lista de tipos de extensões predeterminadas pelo administrador do sistema para os processos de escaneamento;
- 8.1.1.10. A solução em seu processo de escaneamento não deverá comprometer o desempenho computacional do sistema de armazenamento e gerenciamento de dados (NAS);
- 8.1.1.11. Deverá fornecer proteção anti-malware em tempo real para EMC, NetApp, Hitachi e IBM;
- 8.1.1.12. Deverá fornecer suporte CAVA Agent e aos protocolos RPC e ICAP;
- 8.1.1.13. Permitir configurações flexíveis de escaneamento;
- 8.1.1.14. Fornece suporte ao monitoramento de rede via SNMP/MOM;
- 8.1.1.15. Compatibilidade mínima:
 - 8.1.1.15.1. Software:
 - 8.1.1.15.1.1. Microsoft Windows Server 2008/2008 R2 x86/x64 Standard / Enterprise/ Datacenter Edition (incluindo modo Core);
 - 8.1.1.15.1.2. Microsoft Windows Server 2012/2012 R2 Essentials / Standard / Foundation / Datacenter incluindo modo Core);
- 8.1.1.16. Suportar, no mínimo, as Plataformas:
 - 8.1.1.16.1. EMC Celerra / VNX file storages:
 - 8.1.1.16.1.1. EMC DART 6.0.36 ou superior;



prodam

CO-05.06/2021

- 8.1.1.16.1.2. Celerra Antivírus Agent (CAVA) 4.5.2.3 ou superior.
- 8.1.1.16.2. EMC Isilon Storage:
 - 8.1.1.16.2.1. EMC Isilon OneFS 7.0.
- 8.1.1.16.3. EMC NetApp Storages:
 - 8.1.1.16.3.1. NetApp Data ONTAP 7.x e 8.x em 7 mode;
 - 8.1.1.16.3.2. NetApp Clustered Data ONTAP 8.x e 9.x.
- 8.1.1.16.4. IBM Storages:
 - 8.1.1.16.4.1. IBM System Storage N Series;
- 8.1.1.16.5. Hitachi Storages:
 - 8.1.1.16.5.1. HNAS 4100;
 - 8.1.1.16.5.2. HNAS 4080;
 - 8.1.1.16.5.3. HNAS 4060;
 - 8.1.1.16.5.4. HNAS 4040;
 - 8.1.1.16.5.5. HNAS 3090;
 - 8.1.1.16.5.6. HNAS 3080.
- 8.1.1.16.6. NAS:
 - 8.1.1.16.6.1. iCap compatível ou PRC Compatível NAS.
- 8.1.1.16.7. DELL:
 - 8.1.1.16.7.1. DELL FS8600 on FluidFS 6.x;
 - 8.1.1.16.7.2. DELL FS8600 on FluidFS 5.x.
- 8.1.2. Características Mínimas:
 - 8.1.2.1. Proteção anti-malware em tempo real para EMC, NetApp, Hitachi e IBM;
 - 8.1.2.2. Suporte CAVA Agent e aos protocolos RPC e ICAP;
 - 8.1.2.3. Permitir configurações flexíveis de escaneamento;
 - 8.1.2.4. Permitir utilização adaptável dos recursos do sistema;
 - 8.1.2.5. Suporte ao monitoramento de rede via SNMP/MOM;
 - 8.1.2.6. Suportar o gerenciamento dos vírus com base de dados de no mínimo 100 Tb armazenados;
 - 8.1.2.7. Permitir integração com console de gerenciamento centralizado para visualização de relatórios pertinentes as detecções efetuadas nos arquivos armazenados no ambiente NAS;
 - 8.1.2.8. Bloquear malware antes que ele faça seu caminho para seus dispositivos NAS;
 - 8.1.2.9. Verificar arquivos em tempo real quando eles são adicionados ou modificados.
 - 8.1.2.10. Permitir análise dos arquivos armazenados no momento de leitura e gravação no NAS;
 - 8.1.2.11. Suporte ao gerenciamento dos vírus com base de dados de no mínimo 100 Tb armazenados;
 - 8.1.2.12. Permitir integração com console de gerenciamento centralizado para visualização de relatórios pertinentes as detecções efetuadas nos arquivos armazenados no ambiente NAS.



prodam

CO-05.06/2021

9. Suporte Especializado Enhanced Success Plan

9.1. Quantidade: 01 licença

9.1.1. Características Mínimas Exigidas:

9.1.1.1. Todas as licenças deverão acompanhar o serviço de Success Plan, com as seguintes funcionalidades:

- 9.1.1.1.1. Atualização de versões de produtos e correções;
- 9.1.1.1.2. Atualização de mecanismos de varredura (Engine) e assinatura de vacinas (DAT);
- 9.1.1.1.3. Acesso a ferramentas on-line e base de conhecimento o fabricante;
- 9.1.1.1.4. Acesso on-line ao portal de abertura de chamados de suporte do fabricante;
- 9.1.1.1.5. Envio pró-ativo de informativos sobre novas ameaças por e-mail e/ou SMS;
- 9.1.1.1.6. Definição de 25 contatos autorizados do cliente para acesso ao suporte técnico do fabricante, por telefone e portal;
- 9.1.1.1.7. Atendimento telefônico 24x7 por especialista de produtos do fabricante, nestes 36 meses de suporte contratado;
- 9.1.1.1.8. 40 horas contínuas (horário comercial) de consultoria do fabricante da solução;
- 9.1.1.1.9. Um consultor técnico do fabricante realizará análises do ambiente instalado e avaliará a integridade das soluções. Será feita análise de ameaças ao ambiente instalado;
- 9.1.1.1.10. Assistência remota do fabricante;

9.1.1.2. Designação de um Gerente de Sucesso ao Cliente (CSM) no fabricante, o qual realizará:

- 9.1.1.2.1. Ação proativa no quesito segurança, monitorando e fornecimento de revisões de negócios trimestrais;
- 9.1.1.2.2. Conferências telefônicas periódicas com o fabricante para revisão de casos;
- 9.1.1.2.3. Assistência de suporte técnico do fabricante no local conforme necessário para resolver solicitações de serviços críticos de severidades 1, severidade 2 e severidade 3; entende-se por severidade 1 quando há problemas pontuais onde não indisponibilizem serviços críticos definido pela Contratante, severidade 2 quando há indisponibilidade parcial da solução, ou interrupção de algum serviço considerado crítico pela CONTRATANTE, entende-se por severidade 3 quando há indisponibilidade total ou impossibilidade de gerir a solução.



prodam

CO-05.06/2021

- 9.1.1.2.4. no mínimo uma visita semestral on-site à PRODAM para planejamento, avaliação do ambiente instalado e implementação de novos produtos (se necessário); Conferências telefônicas periódicas para revisão de casos;
- 9.1.1.2.5. Relatório periódico de casos fornecidos pelo fabricante;
- 9.1.1.2.6. Processo de escalamento direto com especialista em produtos avançados/desenvolvimento do fabricante;
- 9.1.1.2.7. O suporte mencionado deve ser estendido a todos os produtos do fabricante contratados e utilizados na Empresa;
- 9.1.1.3. Será fornecido pelo fabricante à PRODAM código de acesso ao suporte especializado (Grant Number) em até 10 dias corridos contados a partir da assinatura do contrato.

10. Serviço de Suporte, Manutenção e Garantia

- 10.1. Manutenção das 37.800 licenças no modelo de subscrição da suíte McAfee MV2 – Mvision Protect Plus contendo Antivírus ENS (Endpoint Security), Firewall for Endpoint, Web Control, Device Control, ATP (Adaptive Threat Protection), TIE (Threat Intelligence Exchange), Application Control e ATD (Advanced Threat Defense Applincance) de propriedade da PRODAM, instaladas nas Estações de Trabalho e Servidores localizadas na rede, de propriedade da PRODAM;
- 10.2. Entende-se por serviço de manutenção da suíte antivírus McAfee MV2 – Mvision Protect Plus contendo Antivírus ENS (Endpoint Security), Firewall for Endpoint, Web Control, Device Control, ATP (Adaptive Threat Protection), TIE (Threat Intelligence Exchange), Application Control e ATD (Advanced Threat Defense Applincance), o fornecimento sem ônus das correções de erros e versões atualizadas do software que venham a ser desenvolvidas durante o período de vigência do contrato, das atualizações de assinatura de vírus, bem como do suporte técnico necessário ao perfeito funcionamento do produto na rede da PRODAM;
- 10.3. Os serviços de suporte técnico e garantia abrangem:
 - 10.3.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;
 - 10.3.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente monitorado;
- 10.4. Os serviços de suporte técnico e garantia abrangem todas as soluções fornecidas pela contratada no âmbito dessa contratação;
- 10.5. Os serviços de suporte técnico e garantia de toda a solução deverão ser prestados por um período de 36 (trinta e seis) meses e deverão ser iniciados a partir da data Emissão do Termo de Aceite das licenças adquiridas;



prodam

CO-05.06/2021

- 10.6. Os serviços de suporte técnico poderão ser prestados de forma remota ou presencial (a critério da CONTRATANTE) no endereço da CONTRATANTE (24 x 7), as aberturas de chamados deverão ser por telefone 0800 ou ligação local DDD 011, com resposta inicial em até 2 horas, tanto para severidade 1, 2 ou 3. Entende-se por severidade 1 quando há problemas pontuais onde não indisponibilizem serviços críticos definido pela CONTRATANTE, severidade 2 quando há indisponibilidade parcial da solução, ou interrupção de algum serviço considerado crítico pela CONTRATANTE, entende-se por severidade 3 quando há indisponibilidade total ou impossibilidade de gerir a solução.
 - 10.6.1. O tempo de atendimento para severidade 1 deverá ser em até 24 horas após abertura do chamado;
 - 10.6.2. O tempo de atendimento para severidade 2 deverá ser em até 8 horas após abertura do chamado;
 - 10.6.3. O tempo de atendimento para severidade 3 deverá ser em até 6 horas após abertura do chamado;
- 10.7. Os bens e produtos fornecidos devem ser licenciados de forma que o suporte e a GARANTIA permitam as atualizações dos sistemas e ferramentas durante a vigência do contrato. Deverão estar incluídas tanto as atualizações de segurança, quanto as atualizações para novas versões dos softwares licenciados, atualizações de firmwares, quando disponibilizadas, independente da política de comercialização do fabricante:
 - 10.7.1. Para os servidores fornecidos na solução, a CONTRATADA deve prover GARANTIA de hardware por 36 (trinta e seis) meses dos equipamentos e, caso identifique que o dimensionamento não foi o suficiente deverá providenciar upgrade de componentes, como memória, HD, ou qualquer outro recurso necessário. Caso esse aumento de recursos não seja suficiente, a contratada deverá substituir o servidor por equipamento maior;
 - 10.7.1.1. O prazo máximo para readequação/upgrade/substituição de equipamentos da solução será no máximo de 30 dias após abertura do chamado.
 - 10.7.2. Todas essas correções de infraestrutura devem ser providenciadas sem custo para a CONTRATANTE;
- 10.8. Todos os sistemas ou ferramentas que fazem parte da solução deverão ser disponibilizados na versão mais recente disponibilizada pelo fabricante.
- 10.9. A CONTRATADA deve garantir que todas as personalizações e configurações realizadas sejam automaticamente portadas para novas versões em caso de atualização, reinstalação ou upgrade;
- 10.10. Detalhamento de um plano de ação para correção dos problemas identificados, que será executado pela equipe interna da CONTRATANTE;
- 10.11. A CONTRATADA deverá elaborar, a cada 3 meses, a partir do início do serviço de suporte técnico, relatório sobre a saúde do ambiente da CONTRATANTE utilizando informações fornecidas pela solução contratada. O relatório deve contemplar, no mínimo, as seguintes informações:
 - 10.11.1. Saúde do ambiente de diretório;
 - 10.11.2. Saúde do ambiente de servidores de arquivos;



prodam

CO-05.06/2021

- 10.11.3. Análise de dados coletados para identificar e documentar áreas de risco e vulnerabilidades do ambiente;
- 10.11.4. Evolução em relação a informações de relatórios anteriores;
- 10.12. O relatório descrito no item anterior deverá ser confeccionado e finalizado durante mês em que se completa cada trimestre, contendo no mínimo descrição dos itens 10.11.1, 10.11.2, 10.11.3 e 10.11.4.
- 10.13. A CONTRATADA deverá disponibilizar um especialista técnico na CONTRATANTE uma vez por semana, de forma presencial, para análise do ambiente, discussão e implementação das melhores práticas (a critério da CONTRATANTE, as visitas poderão ser realizadas de forma virtuais devido a pandemia). Esta visita não está associada a visitas técnicas relacionadas com as aberturas de chamados de manutenção e suporte;
- 10.14. É de responsabilidade da CONTRATADA o fornecimento de todo hardware/software necessário para o perfeito funcionamento da solução.

11. Confidencialidade

- 11.1. A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da Contratante para divulgação;
- 11.2. Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (*backdoor*) originadas de *softwares/hardwares* contratado ou adquirido sem o conhecimento e formal autorização da CONTRATANTE. A não observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

12. Obrigações da Contratada

- 12.1. A Contratada deverá oferecer garantia, suporte e licenças da solução e suas funcionalidades contratadas pelo período de 36 meses, a contar da data da assinatura do contrato;
- 12.2. Disponibilizar profissionais certificados pelos fabricantes da solução;
- 12.3. Disponibilizar número de telefone (local ou DDG) para suporte telefônico (24x7x365) e abertura de chamados técnicos;
- 12.4. Ao final da abertura de cada atendimento de suporte, a CONTRATADA deverá emitir um ticket do chamado técnico contendo, no mínimo:
 - 12.4.1. Número do chamado;
 - 12.4.2. Data e hora de abertura do chamado;
 - 12.4.3. Previsão de conclusão do atendimento;
 - 12.4.4. Severidade do erro;
 - 12.4.5. Descrição da solicitação.



prodam

CO-05.06/2021

- 12.5. Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o fechamento deste. Caso a CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, a CONTRATANTE fornecerá as pendências relativas ao chamado aberto.
- 12.6. A CONTRATANTE poderá registrar um número ilimitado de chamados de suporte durante a vigência do Contrato.
- 12.7. Instalação e configuração de todos os hardwares/softwarees descritos neste documento.

13. Acordo Operacional

- 13.1. No intuito de definir procedimentos para o bom andamento das atividades relacionadas neste fornecimento, será definido em até 30 dias corridos após a assinatura do contrato um acordo operacional, neste documento estarão definidos os procedimentos (solicitações, atendimentos, testes, aceites, etc) acordados entre a CONTRATANTE e a CONTRATADA.

14. Prazo de Entrega, Instalação e Ativações

- 14.1. O prazo máximo de entrega das licenças que compõem a solução será de 10 (dez) dias corridos, contados a partir da data de assinatura do contrato.
- 14.2. O prazo máximo de entrega dos servidores para as aplicações, banco de dados e demais serviços, incluindo as licenças de softwares será de 60 (sessenta) dias a corridos, contados a partir da data de assinatura do contrato.
- 14.3. A instalação da solução completa deverá ser feita pela CONTRATADA em conjunto com a CONTRATANTE em até 30 dias corridos após a entrega dos servidores de aplicação, banco de dados e demais serviços.
- 14.4. A instalação será considerada completa quando da migração do atual gerenciamento para a nova infraestrutura contratada, incluindo a gestão dos desktops, servidores, NAS e ativação dos demais serviços definidos neste Termo de Referência. A critério da CONTRATANTE, poderá ser mantido o gerenciamento parcial na solução existente por motivos estratégicos, janelas de migrações, dentre outros motivos de sua responsabilidade.
- 14.5. O projeto de implantação deverá ser entregue em até 60 dias corridos após a assinatura do contrato.
- 14.6. A instalação física e lógica de todos os hardwares/softwarees são de responsabilidade da Contratada.



prodam

CO-05.06/2021

15. Penalidades

- 15.1. Caso haja atraso na entrega código de acesso ao suporte especializado (Grant Number), conforme especificado no item 9.1.1.3, ou as licenças de uso da solução, item 14.1 haverá multa de 1,5% por dia de atraso, calculado sobre o valor do contrato;
- 15.2. Caso haja atraso no período de resposta da abertura de um chamado (2 horas), haverá multa de 0,1% por hora de atraso, calculado sobre o contrato, conforme o item 10.6.
- 15.3. Caso o tempo para atendimento ultrapasse as horas, contadas a partir da abertura do chamado, haverá multa de:
 - 15.3.1. Severidade 1: 0,5% por hora de atraso, calculado sobre o valor mensal do contrato;
 - 15.3.2. Severidade 2: 1% por hora de atraso, calculado sobre o valor mensal do contrato;
 - 15.3.3. Severidade 3: 2% por hora de atraso, calculado sobre o valor mensal do contrato;
- 15.4. Caso haja atraso na disponibilização de profissionais para suporte on site, conforme previsto no item 10.13, haverá multa de 1% ao dia de atraso, calculado sobre o valor mensal do contrato;
- 15.5. Caso haja atraso na entrega dos servidores de aplicação e banco de dados após apresentado o projeto de implantação previsto no item 14.2, haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato;
- 15.6. Caso haja atraso na instalação da solução, conforme previsto no item 14.3, haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato;
- 15.7. Caso não ocorra a visita semestral estabelecido no item 9.1.1.2.4 haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato
- 15.8. Caso não ocorra o upgrade ou substituição dos equipamentos conforme item 10.7.1 haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato.
- 15.9. Caso ocorra atraso na entrega do relatório conforme item 10.12 haverá multa de 0,5% ao dia de atraso, calculado sobre o valor mensal do contrato.

16. Aceite

- 16.1. A equipe técnica da PRODAM emitirá o **Termo de Aceite Final da solução de Suíte Antivírus McAfee MV2 – Mvision Protect Plus** contendo Antivírus ENS (Endpoint Security), Firewall for Endpoint, Web Control, Device Control, ATP (Adaptive Threat Protection), TIE (Threat Intelligence Exchange), Application Control e ATD (Advanced Threat Defense Appliance), de MFE Move AV for Virtual Servers, de MFE VirusScan for Storage para NAS e Suporte Especializado Enhanced Success Plan em até 5 dias úteis após a formalização pela CONTRATADA da finalização do processo de instalação/operação da solução e confirmação que todos os quesitos do Edital foram cumpridos.



prodam

CO-05.06/2021

17. Vigência

18.1. O contrato terá vigência de 36 (trinta e seis) meses, a contar da data de assinatura do Termo de Aceite Final, previsto no item 17.1 deste documento, podendo ser prorrogado até o limite legal de 60 (sessenta) meses, mediante acordo entre as partes, na forma da Lei.



prodam

CO-05.06/2021

ANEXO II

TERMO DE RESPONSABILIDADE DE TERCEIROS E ADESÃO AO CÓDIGO DE CONDUTA E INTEGRIDADE – PRODAM-SP S/A

Nome da empresa: ISH TECNOLOGIA S.A.

CNPJ nº: 01.707.536/0001-04

Nº do contrato de prestação de serviço: CO-05.06/2021

Vigência contratual: 36 (trinta e seis) meses

Objeto contratual: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM FORNECIMENTO DE ATUALIZAÇÕES DE LICENÇAS DE USO PARA 37.000 LICENÇAS DA SUÍTE ANTIVÍRUS MCAFEE MV2 – MVISION PROTECT PLUS, CONTENDO ANTIVÍRUS ENS (ENDPOINT SECURITY), FIREWALL FOR ENDPOINT, WEB CONTROL, DEVICE CONTROL, ATP (ADAPTIVE THREAT PROTECTION), TIE (THREAT INTELLIGENCE EXCHANGE), APPLICATION CONTROL, EPO ON PREMISES, 800 LICENÇAS DE MFE MOVE AV FOR VIRTUAL SERVERS, 1 LICENÇA MFE VIRUSSCAN FOR STORAGE PARA NAS, FORNECIMENTO DE NOVAS LICENÇAS PARA 37.800 ATD (ADVANCED THREAT DEFENSE APPLICANCE), 3 LICENÇAS MFE VIRUSCAN FOR STORAGE PARA NAS, FORNECIMENTO DE 5 SERVIDORES PARA APLICAÇÃO E BANCO DE DADOS, SUPORTE ESPECIALIZADO ENHANCED SUCCESS PLAN E SERVIÇO DE SUPORTE E MANUTENÇÃO PARA TODA A SOLUÇÃO, PELO PRAZO DE 36 MESES.

Declaramos, para os devidos fins, que estamos cientes e concordamos com as normas, políticas e práticas estabelecidas no **CÓDIGO DE CONDUTA E INTEGRIDADE DA PRODAM-SP**, https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/planejamento/prodam/arquivos/governanca/CODIGO%20DE%20CONDUTA%20E%20INTEGRIDADE_v1_2018.pdf, responsabilizando-nos pelo seu integral cumprimento, inclusive por parte dos nossos empregados e prepostos, nos termos do artigo 932, III, do Código Civil, comprometendo-nos com a ética, dignidade, decoro, zelo, eficácia e os princípios morais que norteiam as atividades desempenhadas no exercício profissional e fora dele, em razão das obrigações contratuais assumidas, com foco na preservação da honra e da tradição dos interesses e serviços públicos.

São Paulo/SP, 08 de Junho de 2021.

RENATO TENÓRIO
Procurador

Renato Tenório
Diretor Executivo
RG.: 19.953.787-2
ISH TECNOLOGIA S.A.



prodam

CO-05.06/2021

ANEXO III
MATRIZ DE RISCOS

Risco	Definição	Alocação (público, privado ou compartilhado)	Impacto (alto, médio, baixo)	Probabilidade (frequente, provável, ocasional, remota ou improvável)	Mitigação (medidas, procedimentos ou mecanismos para minimizar)
Mudanças Tributárias	Mudanças na legislação tributária que aumente ou diminua custo, exceto mudança na legislação do IR	Compartilhado	Médio	Remota	Recomposição do equilíbrio econômico financeiro
Capacidade de Pagamento	Redução da capacidade de pagamento da empresa	Privado	Médio	Remota	Antecipação de recebíveis e/ou Aporte de Capital
Variação positiva do dólar	Aumento do preço do dólar muito acima dos índices de inflação previstos para o período.	Compartilhado	Alto	Ocasional	Renegociar contrato ou reduzir escopo de fornecimento ou duração do contrato.
Conflito/guerra (comercial ou armada) envolvendo o país do fabricante	Problemas para manter a solução atualizadas e contatar o fabricante para solucionar bugs e solicitar suporte	Compartilhado	Alto	Improvável	Repactuação do contrato para sua finalização e substituição da solução existente
Governo decretar o fabricante como risco a segurança nacional	Governo proibir a comercialização do produto por entender que há riscos a segurança nacional, envolvendo espionagem nos produtos adquiridos	Compartilhado	Alto	Improvável	Repactuação do contrato para sua finalização e substituição da solução existente



prodam

CO-05.06/2021

Roubo de carga (servidores)	Roubo ou extravio de carga (servidores) durante seu transporte	Compartilhado	Médio	Remota	Manter a solução de servidores existente em produção, até a chegada dos novos equipamentos
Atraso na entrega de servidores	Problemas de importação / liberação da Receita Federal / pandemia	Compartilhado	Médio	Ocasional	Manter a solução de servidores existente em produção, até a chegada dos novos equipamentos

Após 02 (dois) dias da Advertência, mantendo-se o atraso, será aplicada multa de até 1% (um por cento) sobre o valor total do contrato por dia de atraso.

Esses valores devidamente apurados e apresentados à CONTRATADA serão descontados da primeira parcela devida.

Acima de 10 (dez) dias de atraso, fica caracterizada inexecução parcial do Contrato.

Acima de 20 (vinte) dias de atraso, fica caracterizada inexecução total do Contrato.

A natureza da advertência prevista em lei não pode ser abusiva, nem tão pouco configurar um possível desequilíbrio econômico financeiro do termo de contrato que será firmado entre as partes.

Nesta senda, solicitamos uma revisão na cláusula de multas, onde entendemos que os percentuais aplicados são elevados e poderão incidir na parte financeira contratual.

Nossa solicitação será atendida?

RESPOSTA 03:

Não entendemos os percentuais como valores que possam causar desequilíbrio dado os prazos estipulados.

QUESTIONAMENTO 04:

Em atenção aos itens:

7.6. O pagamento será efetuado exclusivamente em conta corrente bancária a ser indicada pela CONTRATADA, a informação deverá ser encaminhada para a Gerência Financeira - GFI, Rua Barão de Itapetininga nº 18 - 4º andar.

7.7. Caso a CONTRATADA solicite que o pagamento seja creditado em conta corrente de outro banco que não o indicado, arcará com todas as despesas e tarifas bancárias vigentes, incorridas na transação de pagamento: DOC, TED, tarifa de emissão de cheque e outras.

Diferentemente do acima exposto, para que haja a identificação do pagamento e baixa automática em sistema dos valores faturados, a liquidação deverá ocorrer através do código de barras que será emitido.

Nesta senda, solicitamos a inclusão nos itens, para que a CET faça o pagamento pela leitura do código de barras.

Nossa solicitação será atendida?

RESPOSTA 04:

O padrão de pagamento da CET é depósito bancário pois em algumas situações ocorrem problemas de medição o que gera problemas de pagamento via boleto bancário, portanto as cláusulas serão mantidas. Contudo, tendo em vista que na solicitação feita a fatura será o próprio boleto e sendo o valor deste correspondente à medição efetuada e ao previsto no contrato, poderá ser realizado o pagamento via código de barras, mediante solicitação apresentada pela Contratada.

QUESTIONAMENTO 05:

Em atenção a CLÁUSULA OITAVA - DO REAJUSTE.

8.1. As parcelas anuais previstas no subitem 7.2 são fixas e irrevogáveis.

Entendemos que pela vigência do termo de contrato (36 meses), a partir do 13º mês de vigência contratual, e dependendo da negociação entre as partes, os valores inicialmente praticados poderão sofrer reajustes.

Nosso entendimento está correto?

RESPOSTA 05:

Não haverá reajuste. Serão 03 parcelas iguais.

14/06/2021

Gerente de Suprimentos

EXPEDIENTE Nº 1818/19

MODALIDADE: PREGÃO ELETRÔNICO Nº 56/20

OBJETO: PRESTAÇÃO DE SERVIÇOS DE IMPLANTAÇÃO DE PADRÃO DE ENTRADA DE ENERGIA NO PAT ESTAIADINHA JULGAMENTO: "MENOR PREÇO TOTAL"

Regime de Execução: Empreitada por Preço Unitário

Encontra-se aberto o PREGÃO acima mencionado, podendo os interessados obter o Edital na Rua Barão de Itapetininga nº 18 - 2º andar - Centro, na Gerência de Suprimentos, de segunda a sexta-feira, no horário das 09h00 às 12h00 e das 14h00 às 17h00, até a data da abertura, mediante a apresentação de mídia eletrônica, ou ainda, no site da Prefeitura do Município de São Paulo - PMSP <http://www.e-negociosciadadep.prefeitura.sp.gov.br>, site da Companhia de Engenharia de Tráfego - CET <http://www.cet.sp.com.br> e no site do Comprasnet www.comprasnet.gov.br.

Os documentos referentes à proposta comercial e anexos (documentos de habilitação) das empresas interessadas deverão ser encaminhados a partir da disponibilização do sistema até as **09h30min do dia 08/julho/2021**, no site www.comprasnet.gov.br. A abertura da Sessão Pública do Pregão Eletrônico, ocorrerá às **09h30min do dia 08/julho/2021**, no site www.comprasnet.gov.br.

Diretor Administrativo e Financeiro

EXPEDIENTE Nº 0509/2020

PREGÃO ELETRÔNICO Nº 49/2020

OBJETO: PRESTAÇÃO DE SERVIÇO DE INFRAESTRUTURA, HARDWARE E LICENCIAMENTO DE USO DO SOFTWARE DE SISTEMA DE CONTROLE OPERACIONAL COM SERVIÇOS DE ATUALIZAÇÃO E ADIÇÃO DE FUNCIONALIDADES NA CENTRAL DE OPERAÇÕES DA CET.

ESCLARECIMENTO Nº 03

Senhores,

Em atenção ao e-mail da empresa interessada em participar do Pregão Eletrônico em referência, após consulta a nossa área técnica e ao nosso jurídico, temos a informar o que segue:

QUESTIONAMENTO 01:

DA OBRIGATORIEDADE DE AGLUTINAR EM UM SÓ ATTESTADO TODA A EXPERIÊNCIA DA LICITANTE.

Item 11.2.4.1.1.1. do Edital: Somente será admitida a apresentação de atestados de objetos diferentes desde que o atestado comprove que cada objeto descrito anteriormente (subitem 11.2.4.1.1.1., letras a até g) corresponda à implantação realizada em um único Contrato.

Não será aceita somatória de atestados para comprovar a capacidade de execução do objeto de um mesmo subitem descrito em 11.2.4.1.1.1.

Respectiva exigência, não estaria afrontando as Leis licitatórias 8.666/93 e 14.133/2021, além do regulamento (RILCC) deste órgão?

QUESTIONAMENTO 02:

Serão aceito atestados de complexidade similar ou superior ou somente especificamente como mencionando no item 11.2.4.1.1?

QUESTIONAMENTO 03:

DA VEDAÇÃO DE CONSÓRCIO:

Outra questão ainda conflitante com as regulamentações atuais e vigentes, tem-se no presente Edital um conflito de aceitação. Ora, não se pode haver, dois pesos e duas medidas. Diante da justificativa prévia no item 17.1 há uma prévia vedação expressa para a aceitação de consórcio, porém, no item 18.1 tem-se a permissão de subcontratação, em total descompasso e conflito com a justificativa utilizada no item 17.1.

Assim, há vedação para participação de consórcio nos itens 3.4 e 4.2 alínea 'a', porém, permite-se a subcontratação, ora se a justificativa para admitir consórcio é que a execução seja realizada pela contratante, então como se pode admitir a subcontratação?

Dessa forma, a fim de aumentar a gama de proponentes, será permitido consórcio?

RESPOSTA 01:

Após consulta a Assessoria Jurídica/CET, informamos que o entendimento não está correto, uma vez que as Leis licitatórias 8.666/93 e 14.133/2021 regulam o regime de contratações da Administração direta, da qual a CET não faz parte.

Conforme item 1.1 do Edital, nosso pregão será processado e julgado em conformidade com a Lei Federal nº 10.520/02, Lei

Federal 13.303/16, com a Lei Complementar nº 123/06 e com o nosso RILCC.

No artigo 47 § 3º do nosso RILCC, a redação é clara sobre a somatória de atestados, estabelecendo que esta regra é uma faculdade.

RESPOSTA 02:

Serão aceitos atestados nos moldes previstos no Edital, e que atendam ao disposto no item 14 do Anexo I - Termo de Referência.

RESPOSTA 03:

Não se verifica condições especiais para indicar a necessidade de participação de consórcios.

Esclarecemos que o software base poderá ser adquirido no mercado, sendo desnecessário que a própria contratada o desenvolva desde o início, o que justifica a subcontratação de 30% do objeto.

No entanto, a realização de melhorias nesse software já existente, para atender às demandas específicas da CET, deve ser feita diretamente pela contratada, conforme item 18 do Anexo I - Termo de Referência.

Ressaltamos que o objetivo da contratação é ter a certeza de adquirir algo já testado e aprovado pelo mercado, não sofrendo com o desenvolvimento do zero de um software embrionário e ter a agilidade para implementação e uso do mesmo.

A certeza de que o software base ofertado pelo licitante vencedor do certame, na fase de habilitação e preço, está apto a ser contratado, será dada quando o sistema for testado e aprovado atendendo ao descrito no Anexo I - Termo de Referência, conforme item 12 TESTES DE PROVA DE CONCEITO DO SISTEMA PARA A CONTRATAÇÃO.

GSP, 14/06/2021.

Gerente de Suprimentos

EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

GABINETE DO PRESIDENTE

EXTRATO DE TERMO DE CONTRATO

CO-04.06/2021

PROCESSO SEI Nº 7010.2021/0000053-6

PREGÃO ELETRÔNICO Nº 01.001/2021

CONTRATANTE: EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO

— PRODAM-SP S/A.

CONTRATADA: DECISION SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO LTDA.

CNPJ Nº 03.535.902/0002-00

OBJETO: CONTRATAÇÃO DE EMPRESA PARA FORNECIMENTO DE SOLUÇÃO DE INFRAESTRUTURA COMPUTACIONAL HIPERCONVERGENTE COMO SERVIÇO, CONTEMPLANDO HARDWARE E SUPORTE TÉCNICO.

VIGÊNCIA: 60 (SESSENTA) MESES, CONTADOS A PARTIR DA DATA DO "TERMO DE ACEITE FINAL".

VALOR: R\$ 6.978.009,60 (SEIS MILHÕES, NOVECIENTOS E SETENTA E OITO MIL, NOVE REAIS E SESSENTA CENTAVOS).

CO-05.06/2021

PROCESSO SEI Nº 7010.2021/0004904-7

PREGÃO ELETRÔNICO Nº 05.002/2021

CONTRATANTE: EMPRESA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO MUNICÍPIO DE SÃO PAULO

— PRODAM-SP S/A.

CONTRATADA: ISH TECNOLOGIA S/A.

CNPJ Nº 01.707.536/0001-04

OBJETO: CONTRATAÇÃO DE EMPRESA ESPECIALIZADA EM FORNECIMENTO DE ATUALIZAÇÕES DE LICENÇAS DE USO PARA 37.000 LICENÇAS DA SUÍTE ANTIVÍRUS MCAFEE MV2 — MVISION PROTECT PLUS CONTENDO ANTIVÍRUS ENS (END-POINT SECURITY), FIREWALL FOR ENDPOINT, WEB CONTROL, DEVICE CONTROL, ATP (ADAPTIVE THREAT PROTECTION), TIE (THREAT INTELLIGENCE EXCHANGE), APPLICATION CONTROL, EPO ON PREMISES, 800 LICENÇAS DE MFE MOVE AV FOR VIRTUAL SERVERS, 1 LICENÇA MFE VIRUSSCAN FOR STORAGE PARA NAS, FORNECIMENTO DE NOVAS LICENÇAS PARA 37.800 ATD (ADVANCED THREAT DEFENSE APPLICATIONCE), 3 LICENÇAS MFE VIRUSSCAN FOR STORAGE PARA NAS, FORNECIMENTO DE 5 SERVIDORES PARA APLICAÇÃO E BANCO DE DADOS, SUPORTE ESPECIALIZADO ENHANCED SUCCESS PLAN E SERVIÇO DE SUPORTE E MANUTENÇÃO PARA TODA A SOLUÇÃO, PELO PRAZO DE 36 MESES.

VIGÊNCIA: 36 (TRINTA E SEIS) MESES, A CONTAR DA DATA DE ASSINATURA DO TERMO DE ACEITE FINAL, PREVISTO NO ITEM 16.1 DO TERMO DE REFERÊNCIA.

VALOR: R\$ 13.120.000,00 (TREZE MILHÕES, CENTO E VINTE MIL REAIS).

SÃO PAULO URBANISMO

GABINETE DO PRESIDENTE

PROCESSO SEI Nº 7810.2017/0000390-1

RESOLUÇÃO DE DIRETORIA RD Nº DAF 02/2021

ASSUNTO: Autorização para prorrogação por mais 90 dias do Contrato nº 7810.2017/0000390-1, Processo SEI nº 7810.2017/0000390-1, firmado com a empresa SODEXO PASS DO BRASIL SERVIÇOS E COMÉRCIO S/A. para prestação de serviços de administração e gerenciamento de créditos disponibilizados em cartão eletrônico com chip, de vale refeição e vale alimentação, para utilização pelos empregados e estagiários da SPURBANISMO.

A Diretoria Executiva, apreciando o exposto pelo Diretor Relator, em observância ao art. 57, II, da Lei Federal nº 8.666/93 c/c o art. 91, § 3º, da Lei Federal nº 13.303/2016, e considerando a manifestação de DAF/GCL sob o evento nº 045946091 e o Parecer Jurídico nº 045957043 favorável e exarado nos autos eletrônicos SEI nº 7810.2017/0000390-1:

RESOLVE:

I - AUTORIZAR a prorrogação do prazo do Contrato nº 7810.2017/0000390-1, Processo SEI nº 7810.2017/0000390-1, firmado entre a SP-Urbanismo e a empresa SODEXO PASS DO BRASIL SERVIÇOS E COMÉRCIO S/A., CNPJ/MF nº 69.034.668/0001-56, para prestação de serviços de administração e gerenciamento de créditos disponibilizados em cartão eletrônico com chip, de vale refeição e vale alimentação, para utilização pelos empregados e estagiários da SP-URBANISMO, por um período de 90 (noventa) dias ou, até o início da prestação de serviços por empresa a ser selecionada em procedimento licitatório, o que ocorrer primeiro;

- PERÍODO DE VIGÊNCIA: de 16/06/2021 até 14/09/2021;

- VALOR DO CONTRATO: R\$ 494.797,44 (quatrocentos e noventa e quatro mil, setecentos e noventa e sete reais e quarenta e quatro centavos);

- RESERVA ORÇAMENTÁRIA, documento SEI 045437980;

- IDENTIFICAÇÃO DA DOTAÇÃO

Programática: 15.122.3024.2.100

Despesa: 3.3.90.46.00

Fonte de Recursos: 09

II - EMPENHO: Em decorrência, emita-se nota de empenho no valor de R\$ 494.797,44 (quatrocentos e noventa e quatro mil, setecentos e noventa e sete reais e quarenta e quatro centavos), demais empenhos e cancelamentos que vierem a ocorrer no exercício de 2021, em favor da empresa SODEXO

PASS DO BRASIL SERVIÇOS E COMÉRCIO S/A., CNPJ/MF nº 69.034.668/0001-56, com fundamento legal nas Leis Federais 13.303/2016, 4.320/1964 e suas alterações e na legislação municipal vigente.

III - FISCAL DO CONTRATO: Sra. Valdete Alves de Oliveira Soares

IV - DETERMINAR que a Gerência de Compras, Licitações e Contratos da

Diretoria Administrativa e Financeira adote as providências necessárias para o cumprimento da presente Resolução.

SÃO PAULO OBRAS

GABINETE DO PRESIDENTE

EXTRATO DO ADITAMENTO Nº 01 AO CONTRATO Nº 0452030100 – PROCESSO SEI Nº 7910.2020/0000468-0

Objeto Prestação de serviços de limpeza, asseio e conservação predial, com fornecimento de mão de obras, saneantes domissanitários, materiais e equipamentos, visando à obtenção de adequadas condições de salubridade e higiene, serviços de copa e auxiliares de serviços gerais, todos sob a inteira responsabilidade da Contratada.

Contratada: BON GOURMET SERVIÇOS LTDA. – BGS

CNPJ: 08.252.332/0001-75

Objeto do aditamento: Fica acordada entre as partes a redução de 10% (dez por cento) do valor apropriado para horas extras, a partir de 01.06.2021. Com o referido desconto o valor do saldo do contrato P0 passa de R\$ 864.545,02, (oitocentos e sessenta e quatro mil, quinhentos e quarenta e cinco reais e três mil, setecentos e nove reais e oitenta e dois centavos).A Contratada, neste ato, em face da renegociação do contrato, renuncia, expressamente, ao reajuste contratual previsto para o mês de setembro de 2021, sem qualquer direito a pedido de indenização relativo a este período. Fica, ainda, ajustado entre as partes que em razão do quanto disposto no art. 6º do Decreto nº. 60.041/2020, que a data-base do Contrato passa a ser abril de 2021 para efeito de aplicação de reajuste contratual.

Data da assinatura: 01/06/2021

EXTRATO DO ADITAMENTO Nº 02 AO CONTRATO Nº 018183010

PROCESSO SEI Nº 7910.2017/0000626-2

Objeto do contrato Prestação de serviços para desenvolver, implantar e executar os serviços relativos ao PROGRAMA DE CONTROLE MÉDICO DE SAÚDE OCUPACIONAL – PCMSO – NR7 e ao PROGRAMA DE PREVENÇÃO DE RISCOS AMBIENTAIS – PPRR – NR9, conforme previsto na legislação trabalhista, Portaria nº 3.214, de 8 de junho de 1978, especialmente as Normas Regulamentadoras NR7 e NR9 do Ministério do Trabalho e Emprego, e fixadas no Termo de Referência.

Contratada: ACG Assessoria Ocupacional Ltda-ME.

CNPJ: nº 11.383.444/0001-70

Objeto do aditamento: A Contratada, em face da renegociação do contrato, renunciou, expressamente, ao reajuste contratual para o mês de março de 2021, sem qualquer direito a pedido de indenização relativo a este período. Fica, ainda, ajustado entre as partes, em razão do quanto disposto no art. 6º do Decreto nº. 60.041/2020, que a data-base do Contrato passa a ser abril de 2021 para efeito de aplicação de reajuste contratual.

Data: 11/06/2021

SÃO PAULO TRANSPORTE

GABINETE DO PRESIDENTE

GERÊNCIA DE CONTRATAÇÕES ADMINISTRATIVAS

LICITAÇÃO Nº 007/2021

AVISO

A SÃO PAULO TRANSPORTE S/A – SPTrans, inscrita no CNPJ-MF sob o nº 60.498.417/0001-58, comunica que se encontra aberta a LICITAÇÃO, pelo rito da modalidade PREGÃO na forma ELETRÔNICA, através do modo de disputa aberto, do tipo menor preço sob nº 007/2021, vinculado ao PÁLC nº 2021/0222 e será regido pela Lei Federal no 13.303, de 30/06/16, Lei Complementar nº 123, de 14/12/06 e alterações; Decreto Municipal nº 56.475, de 05/10/15; Lei Municipal no 14.094, de 06/12/05 e Regulamento Interno de Licitações e Contratos da SPTrans - RILC, disponível no link http://www.sptrans.com.br/media/1158/regulamento_interno_licitacoes_e_contratos_out18.pdf, que foi publicado no Diário Oficial da Cidade em 18/10/18, bem como demais diplomas aplicáveis à espécie e disposições do Edital.

OBJETO: AQUISIÇÃO DE ATIVOS DE REDE - 02 (DOIS) SWITCHES SAN DE 24 PORTAS LICENCIADAS CADA UM, COM FORNECIMENTO DE 48 TRANSCEIVERS ÓPTICO FIBRE CHANNEL SFP+ SWL DE 16GBPS PARA OS SWITCHES SAN E FORNECIMENTO DE 48 CORDÕES ÓPTICOS DUPLEX DE FIBRA (MM) MULTIMODO OM3 COM CONECTORES LC X LC (MACHOS) COM 50/125 MICRONS E 15 METROS DE COMPRIMENTO.

Limite para recebimento das propostas: 28/06/2021 às 10h, por meio da página eletrônica www.licitacoes-e.com.br

Abertura das propostas: 28/06/2021 às 10h.

Início da Disputa de Preços (Pregão): 28/06/2021 às 10h15.

Os interessados poderão obter gratuitamente os arquivos eletrônicos com a íntegra do edital e seus anexos, no site www.licitacoes-e.com.br e no site www.sptrans.com.br dentro do "link" Licitações.

Alternativamente, os mesmos arquivos eletrônicos poderão ser obtidos diretamente na SPTrans, mediante a entrega de um exemplar de CD-ROM do tipo CDR-80, virgem e lacrado.

A retirada do edital gravado em CD-ROM será feita na Gerência de Contratações Administrativas – DA/SAM/GCA da SPTrans, localizada na Rua Boa Vista, nº 236 – 2º andar – Centro – São Paulo/SP, de segunda a sexta-feira, no horário entre 9h e 12h e 14h e 17h.

São Paulo, 14 de junho de 2021.

Jomar Santos de Lisboa

Pregoeiro

TRIBUNAL DE CONTAS

GABINETE DO PRESIDENTE

EXTRATO DE TERMO DE CONTRATO

TERMO DE CONTRATO: Nº 09/2021

CONTRATANTE: TRIBUNAL DE CONTAS DO MUNICÍPIO DE SÃO PAULO

CONTRATADA: SIMPRESS COMÉRCIO, LOCAÇÃO E SERVIÇOS LTDA

CNPJ: 07.432.517/0001-07

OBJETO DO CONTRATO: Serviços de Solução de Impressão e Escaneamento Departamental, com Software de Gerenciamento via Rede Local (TCP/IP).

VALOR CONTRATUAL: R\$ 984.399,36

DOTAÇÃO: 10.10.01.032.3024.2818.3390.40

PROCESSO TC: Nº 005616/2021

PRAZO DE VIGÊNCIA: 48 meses

DATA DA ASSINATURA: 14/06/2021

DESPACHO DA CHEFE DE GABINETE DA PRESIDÊNCIA

TC/ 012255/2017

Interessados: TCMSP / UPLEXIS TECNOLOGIA LTDA

Objeto: Autorização

DESPACHO: À vista das informações constantes dos autos, notadamente das manifestações da Subsecretaria Administrativa e da Secretaria Geral, que acolho como razões de decidir, nos termos da competência delegada pela Portaria SG/GAB nº 03/2019, AUTORIZO, com fundamento no artigo 57, inciso IV, da Lei Federal nº 8.666/1993, no artigo 46 do Decreto Municipal nº 44.279/2003, assim como na Subcláusula IV.1 da Cláusula IV do Termo de Contrato nº 11/2018, tendo por objeto a locação de licença de uso do Sistema UpMiner – Mineração de dados e atualizações, com vigência até 31/07/2021, a adoção das seguintes providências: I) Prorrogação do Contrato nº 11/2018, firmado com a empresa UPLEXIS TECNOLOGIA LTDA., CNPJ nº 06.242.066/0001-74, pelo prazo de 12 (doze) meses, no período compreendido entre 01/08/2021 a 31/07/2022. II) Emissão de notas de empenho, pagamento e cancelamento do saldo, se houver, em favor da referida empresa, no valor total estimado de R\$ 34.896,96 (trinta e quatro mil, oitocentos e noventa e seis reais e noventa e seis centavos), devendo onerar a dotação 10.10.01.032.3024.2818.3390.40 – Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica. III) Lavratura do Termo de Aditamento, conforme minuta encartada como peça 748.

DESPACHO DA CHEFE DE GABINETE DA PRESIDÊNCIA

TC/ 005290/2021

Interessados: TCMSP / FINO SABOR INDÚSTRIA E COMÉRCIO LTDA