MARIA DE LOURDES LEIRIA
30/09/2021 15:16

HELIO FERREIRA DA SILVA JUNIOR
04/10/2021 12:05

TERMO DE CONTRATO – RP 9019/2021

Termo de contrato de aquisição de solução de segurança de *endpoints,* que entre si celebram o **Tribunal Regional do Trabalho da 12ª Região** e a empresa **ISH Tecnologia S/A**

CONTRATANTE: A União, por meio do **Tribunal Regional do Trabalho da 12ª Região**, estabelecido na rua Esteves Júnior, n° 395, bairro Centro, na cidade de Florianópolis, Estado de Santa Catarina, CEP 88015-905, inscrito no CNPJ sob o n° 02.482.005/0001-23, neste ato representado por sua Desembargadora do Trabalho-Presidente, Exma. Senhora **Maria de Lourdes Leiria**.

CONTRATADA: A empresa **ISH Tecnologia S/A**, inscrita no CNPJ/MF sob o nº 01.707.536/0001-04, estabelecida na rua Judith Maria Tovar Varejão, nº 355, bairro Enseada do Suá, na cidade de Vitória, Estado do Espírito Santo, CEP 29050-360, telefone (27) 3334-8900, e-mail helio.ferreira@ish.com.br, neste ato representada por seu representante legal, Senhor **Hélio Ferreira da Silva Júnior**, portador do RG sob nº 2.107.159, emitido pela SSP/DF e do CPF sob nº 003.868.541-81.

Os CONTRATANTES resolvem celebrar o presente contrato tendo em vista o que consta do Protocolo Administrativo TRT13 nº 19.251/2021, da Ata de Registro de Preços nº 05/2021 do Pregão Eletrônico n° 11/2021 do TRT da 13ª Região, e mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA – DOS FUNDAMENTOS LEGAIS DO CONTRATO

O presente Contrato fundamenta-se:

I. Nos termos propostos pela CONTRATADA que, simultaneamente:

a) constem no **Protocolo Administrativo TRT13 nº 19.251/2021,**

b) não contrariem o interesse público;

II. Nas determinações da Lei n.º 8.666/93;

III. Nos preceitos de direito público;

IV. Supletivamente, nos princípios da teoria geral dos contratos e nas disposições do direito privado;

V. Nas determinações da Lei 10.520/2002, de 17 de julho de 2002, e pela regulamentação dada pelo Decretos no 10.024/2019, n° 7.892/2013 e suas alterações, bem como a Lei Complementar N° 123/2006, alterada pela Lei Complementar n° 147/2014, Lei Complementar n.° 155/2016, Decreto n° 8.538/2015 e ainda pelas condições e exigências estabelecidas no Edital;

VI. Na Ata de Registro de Preços TRT13 nº 05/2021.

CLÁUSULA SEGUNDA – DO OBJETO

2.1. A presente contratação consiste na aquisição de licença de uso com serviço de suporte e direito de atualização para solução de antivírus, do tipo *endpoint*, com licenciamento, instalação, capacitação e suporte técnico pelo período de 48 (quarenta e oito) meses, por meio da ARP nº 05/2021 do TRT13, que o TRT12 é participante.

2.2. Os serviços devem ser prestados contínua e ininterruptamente, durante a vigência do contrato, obedecidos aos prazos e procedimentos especificados nos Níveis de Serviço.

2.3. Os serviços serão realizados mediante acesso remoto aos servidores de aplicação e às estações de trabalho dos usuários. Caso não seja possível via acesso remoto, os serviços deverão ser prestados presencialmente nas dependências do TRT 12ª Região ou, eventualmente, em local a ser indicado por este Tribunal na mesma cidade de sua sede, sendo que os custos para a prestação presencial dos serviços correrão por conta da CONTRATADA.

CLÁUSULA TERCEIRA – DA ESPECIFICAÇÃO DA SOLUÇÃO

3.1. As especificações técnicas da solução objeto deste Contrato constam no Termo de Referência (anexo I do Edital do Pregão Eletrônico nº 11/2021 do TRT13), constante no Protocolo TRT nº 19.251/2021, que independentemente de transcrição, é parte integrante deste Contrato.

3.1.1 Especificações completas referentes a solução de Software de segurança (antivírus) para *endpoints* (estações de trabalho, dispositivos móveis e servidores físicos, incluindo capacitação e instalação), constam do Anexo I deste termo.

CLÁUSULA QUARTA – DAS OBRIGAÇÕES DO CONTRATANTE

São obrigações do CONTRATANTE:

4.1. Proporcionar todas as condições para que a CONTRATADA possa desempenhar as atividades de acordo com as determinações do Contrato e do Termo de Referência do Edital do Pregão Eletrônico nº 11/2021, que resultou na ARP 05/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante;

4.2. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais;

4.3. Notificar a CONTRATADA, por escrito, da ocorrência de eventuais imperfeições na prestação dos serviços, fixando prazo para a sua correção, caso não previsto neste instrumento;

4.4. Zelar para que sejam mantidas, em compatibilidade com as obrigações assumidas pela CONTRATADA, todas as condições de habilitação e qualificação exigidas na contratação;

4.5. Fornecer atestados de capacidade técnica, quando solicitado pela CONTRATADA, desde que atendidas às obrigações;

4.6. Emitida a Nota de Empenho, o Contratante deverá remeter cópia deste, bem como “termo de contrato” à CONTRATADA, via e-mail institucional, objetivando ciência do procedimento de contratação e assinatura do referido termo;

4.7. Para fins de formalização do ato de recebimento dos supramencionados documentos, de forma idêntica, a CONTRATADA deverá informar a sua recepção;

4.8. Prestar as informações e os esclarecimentos atinentes ao objeto que venham a ser

solicitados pela CONTRATADA;

4.9. Efetuar o pagamento à CONTRATADA nos termos previstos em Contrato;

4.10. Nomear Gestor e Fiscais Técnico e Administrativo para acompanhar e fiscalizar a execução do contrato;

4.11. Receber os serviços prestados pela CONTRATADA desde que esteja em conformidade com o definido no contrato;

4.12. Emitir pareceres no processo administrativo relativo à presente contratação, especialmente quanto à aplicação de penalidades e alterações contratuais, pelos gestores do contrato.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

Além de entregar o objeto contratado conforme as especificações técnicas, pelo preço selecionado, no prazo acordado e no local indicado no Termo de Referência do Edital do Pregão Eletrônico nº 11/2021, que resultou na ARP 05/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante, parte integrante deste contrato independente de transcrição, são obrigações da CONTRATADA:

5.1. Atender prontamente quaisquer orientações e exigências do Gestor do Contrato, inerentes à execução do objeto contratual;

5.2. Coordenar, sob sua exclusiva responsabilidade, os profissionais necessários à prestação dos serviços objeto desta contratação;

5.3. Designar formalmente preposto, apto a representá-la junto ao Contratante, em até 2 dias úteis da assinatura do Contrato;

5.4. Cumprir o Acordo de Nível de Serviço (SLA) estabelecido na seção 15.4 (“Níveis de Serviço”) do Termo de Referência do Edital do Pregão Eletrônico nº 11/2021, que resultou na ARP 05/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante;

5.5. Submeter à aprovação do CONTRATANTE toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo ou legal;

5.6. Responsabilizar-se por todos os encargos sociais, trabalhistas, previdenciários, fiscais e comerciais, tributos de qualquer espécie que venham a ser devidos em decorrência da execução deste instrumento, bem como custos relativos ao deslocamento e à estada de seus profissionais, caso existam;

5.7. Responsabilizar-se pelos danos causados diretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo, ação ou omissão, quando da execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento realizado pelo CONTRATANTE;

5.8. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais, em consequência de fato a ela imputável e relacionado com esta contratação;

5.9. Arcar com todos os prejuízos advindos de perdas e danos, incluindo despesas judiciais e honorários advocatícios resultantes de ações judiciais, a que o CONTRATANTE for compelido a responder em decorrência desta contratação;

5.10. Manter seus funcionários, quando nas dependências do CONTRATANTE, sujeitos às normas internas deste (segurança e disciplina), porém sem qualquer vínculo empregatício com o Órgão;

5.11. Possibilitar a fiscalização do CONTRATANTE, no tocante à verificação das especificações exigidas no Termo de Referência do Edital do Pregão Eletrônico nº 11/2021, que resultou na ARP 05/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram;

5.12. Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada, para a adoção das medidas necessárias à sua regularização;

5.13. Manter as condições de habilitação consignadas no Edital de Licitação e anexos do Pregão Eletrônico nº 11/2021, que resultou na ARP 05/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante;

5.14. Não transferir a terceiro, no todo ou em parte, o objeto da presente contratação;

5.15. Para fins de comunicação entre as partes contratantes, eventuais mudanças de endereço e correio eletrônico da Contratada deverão ser comunicadas ao Contratante, no prazo de **05 (cinco) dias úteis**;

5.16. A CONTRATADA deverá observar a previsão contida no art. 2º, inc. VI, da Resolução CNJ nº 07/2005, alterada pela Resolução CNJ nº 229/2016, o qual dispõe sobre a vedação nas contratações, independentemente da modalidade de licitação, de pessoa jurídica que tenha em seu quadro societário cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, dos magistrados ocupantes de cargos de direção ou no exercício de funções administrativas, assim como de servidores ocupantes de cargos de direção, chefia e assessoramento vinculados direta ou indiretamente às unidades situadas na linha hierárquica da área encarregada da licitação, apresentando declaração de conformidade;

5.17. Adotar os critérios de sustentabilidade, constantes do subitem 5.2.1 Serviços que envolvam a utilização de mão de Obra, residente ou não, do Guia de Contratações Sustentáveis da Justiça do Trabalho, instituído pela Resolução nº 103/2012 do Conselho Superior da Justiça do Trabalho;

5.18. Apresentar declaração de que não emprega menores de 18 anos em trabalho noturno, perigoso ou insalubre, e de qualquer trabalho a menores de 16 anos, salvo na condição de aprendiz, a partir de 14 anos, conforme disposto no inc. V do art. 27 da Lei nº 8.666;

5.19. A Contratada deverá observar a previsão contida no art. 5º, inc. IV da Lei nº 12.846/2013, a qual dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira;

5.20. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, as partes do objeto deste contrato em que se verificarem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços;

5.21. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do CONTRATANTE, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos;

5.22. Não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTE/SDH no 2, de 12 de maio de 2011;

5.23 Não ter sido condenada, a empresa ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou gênero, ao trabalho infantil e ao trabalho escravo, em afronta à previsão aos artigos 1º e 170 da Constituição Federal de 1988, do artigo 149 do Código

Penal Brasileiro; do Decreto nº 5.017, de 12 de março de 2004 (promulga o Protocolo de Palermo) e das Convenções da OIT nºs 29 e 105.

CLÁUSULA SEXTA – DA TRANSFERÊNCIA DE CONHECIMENTO, DO SIGILO E DO MODELO DE EXECUÇÃO E DE GESTÃO DO CONTRATO

6.1. Encontram-se detalhadas no Item 15 do Termo de Referência do Edital do Pregão Eletrônico TRT13 nº 11/2021 as regras relativas à(o):

- Modelo de execução e de gestão do contrato.
- Transferência de conhecimento; e
- Propriedade, sigilo e restrições.

CLÁUSULA SÉTIMA – DO VALOR, DO REAJUSTE E DAS ALTERAÇÕES DO CONTRATO

7.1. Pelo objeto do presente Contrato, o CONTRATANTE pagará à CONTRATADA o **valor** de **R$ 79.328,80 (setenta e nove mil, trezentos e vinte e oito reais e oitenta centavos) para o exercício 2021 (meses out/nov/dez)**, estando nele incluídos todos os tributos, bem como quaisquer outras despesas, inclusive frete, pela solução (que inclui gerenciamento, garantia, atualizações, suporte técnico, manutenção preventiva e corretiva), conforme abaixo especificado:

GRUPO ÚNICO

ITEM	DESCRIÇÃO	QTD.	P. UNIT. LICENÇA/MÊS	TOTAL EXERCÍCIO 2021 (out/nov/dez)	SD
1	Licença de software de segurança para estações de trabalho (endpoints) e servidores + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	3.000	2,616	23.544,00	11
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	100	2,616	784,80	11
3	Implantação e configuração da solução + Repasse de conhecimento hands-on.	1	16.000,00	16.000,00	21
4	Treinamento EAD de capacitação técnica para administração da solução.	15	2.600,00	39.000,00	20

7.2. Os preços dos serviços correspondentes aos itens 1 e 2 objeto deste contrato, cujo pagamento é mensal, desde que observado o interregno mínimo de **12 (doze) meses**, contado da data limite para apresentação da proposta de preços pela licitante ou, nos reajustes subsequentes ao primeiro, da data de início dos efeitos financeiros do último reajuste ocorrido, poderão ser reajustados utilizando-se a variação do Índice de Custos de Tecnologia da Informação – ICTI, nos termos da Portaria nº 6.432, de 11 de julho de 2018,

publicada em 13/07/2018 no Diário Oficial da União – DOU, acumulado em 12 (doze) meses, cuja formalização ocorrerá por simples apostilamento, na forma da legislação atinente à matéria. Os preços dos itens 3 e 4, cujo pagamento será em parcela única, são irreajustáveis;

7.3. A CONTRATADA fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões no objeto contratado, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato (art. 65, § 1.º, da Lei n.º 8.666/93).

7.4. O Contrato poderá ser alterado, devidamente justificado, na hipótese de ocorrência de situação prevista no art. 65 da Lei n.º 8.666/93.

CLÁUSULA OITAVA – DAS CONDIÇÕES DE FORNECIMENTO DO SERVIÇO E DO RECEBIMENTO

8.1. A entrega do objeto deverá ocorrer no prazo, características e condições estabelecidas no Termo de Referência, Anexo I do Edital de Licitação nº 11/2021 do TRT13, que independente de transcrição é parte integrante deste Contrato.

8.2. A CONTRATADA deverá cumprir os eventos descritos nas tabelas a seguir, respeitando os prazos máximos estabelecidos, os quais poderão ser antecipados sempre que as circunstâncias assim o permitam:

MARCO	PRAZO (dias úteis)	EVENTO	RESPONSÁVEL
D0	-	Assinatura do contrato	TRT12 e CONTRATADA
D1	D0+10	Reunião de Planejamento	TRT12 e CONTRATADA
D2	D0+20	Instalação e configuração da solução	CONTRATADA
D3	D2+05	Recebimento Provisório	TRT12
D4	D3+05	Recebimento Definitivo	TRT12

8.3. Caso a empresa verifique a impossibilidade de cumprir com os prazos estabelecidos, deverá encaminhar ao CONTRATANTE solicitação de prorrogação de prazo, da qual deverão constar:

a. Motivo do não cumprimento do prazo, devidamente comprovado, e o novo prazo previsto para entrega;

b. A comprovação de que trata esta cláusula deverá ser promovida não apenas pela alegação da empresa CONTRATADA, mas por meio de documentos que relatem e justifiquem a ocorrência que ensejar o descumprimento de prazo, tais como: carta do fabricante/fornecedor, laudo técnico de terceiros, Boletim de Ocorrência de Sinistro, ou outro equivalente.

8.4. A solicitação de prorrogação de prazo será analisada pelo CONTRATANTE na forma da lei e de acordo com os princípios de razoabilidade e proporcionalidade, informando-se à empresa da decisão proferida. Em caso de denegação da prorrogação do prazo de entrega, e caso não cumpra o prazo inicial, o fornecedor ficará sujeito às penalidades previstas para atraso na entrega.

8.5. Para todos os efeitos, a conclusão da entrega do objeto será dada pela entrega da

solução em pleno funcionamento, conforme avaliado pela equipe técnica do CONTRATANTE.

8.6. O recebimento do objeto se dará da seguinte forma:

a) **Recebimento Provisório (item 3):** instalação e configuração do console de gerência da solução e repasse de conhecimento hands-on aos servidores do CONTRATANTE;

b) **Recebimento Definitivo (item 3):** verificação do perfeito funcionamento do console. O recebimento deste item autoriza o início do faturamento dos itens 1 e 2;

c) **Recebimento Provisório (mensal - itens 1 e 2):** entrega do relatório de chamados atendidos no mês, contendo a descrição, a solução adotada e as datas de abertura, conclusão do chamado e responsáveis pela abertura e conclusão, bem como serviços prestados eventual e proativamente;

d) **Recebimento Definitivo (mensal - itens 1 e 2):** verificação dos serviços prestados e sua aderência às condições estabelecidas no Termo de Referência (Anexo I do Edital de Licitação nº 11/2021 do TRT13);

e) **Recebimento Provisório (item 4):** conclusão do treinamento para os servidores do CONTRATANTE;

f) **Recebimento Definitivo (item 4):** avaliação satisfatória do treinamento por, pelo menos, 80% dos participantes do treinamento.

8.7. O Termo de Recebimento Definitivo deverá ser emitido em até **05 (cinco) dias úteis**, contados do recebimento provisório.

8.8. O recebimento definitivo não exclui a responsabilidade da CONTRATADA pela qualidade e execução dos serviços durante a vigência do contrato, ainda que vícios e desconformidades com as especificações técnicas sejam verificadas posteriormente ao recebimento.

8.9. Caso sejam constatadas inadequações, atrasos, falhas ou incorreções no objeto, a CONTRATADA será notificada e obrigada a efetuar as correções necessárias, sem ônus para o CONTRATANTE, no prazo de **5 (cinco) dias úteis**. Essa notificação interrompe os prazos de recebimento e de pagamento até que a irregularidade seja sanada e ratificada.

CLÁUSULA NONA – DO NÍVEL DE SERVIÇO

9.1. Os níveis de serviço serão exigidos de acordo com o disposto no item 15.4. do Termo de Referência, Anexo I do Edital de Licitação nº 11/2021 do TRT13, que é parte integrante do Edital e deste instrumento, independente de transcrição.

CLÁUSULA DEZ – DA DOTAÇÃO ORÇAMENTÁRIA E RETIRADA DO EMPENHO

10.1 Os recursos necessários à execução deste contrato correrão à conta dos recursos orçamentários consignados ao CONTRATANTE na Classificação da Despesa: 33.90.40.11 - Suporte de Infraestrutura de TIC (itens 1 e 2), 33.90.40.21 - Serviços Técnicos de Profissionais de TIC – PJ (item 3) e 33.90.40.20 - Treinamento/Capacitação em TIC (item 4) e constante do Programa de Trabalho 02.122.0033.4256.0042.0001 – Manutenção e Gestão dos Serviços de Tecnologia da Informação, sendo emitida, pelo CONTRATANTE, para cobertura das despesas relativas ao presente contrato, a Nota de Empenho n.º 2021NE403, datada de 28/09/2021, no valor de R$ 79.328,80 (setenta e nove mil, trezentos e vinte e oito

reais e oitenta centavos).

CLÁUSULA ONZE – DO PAGAMENTO

11.1. Os pagamentos serão efetuados em moeda corrente nacional, até o 10° (décimo) dia útil após a emissão do Termo de Recebimento Definitivo pelo Gestor do Contrato. Todo e qualquer pagamento será mediante Ordem Bancária emitida em nome do fornecedor e creditada em sua conta-corrente que deverá estar especificada no corpo na referida Nota Fiscal, ou por meio de ordem bancária para pagamento de faturas em código de barras;

11.1.1. Para os **itens 1 e 2**, o pagamento será efetuado em **48 (quarenta e oito) parcelas mensais**;

11.1.2. Para os **itens 3 e 4**, o pagamento será efetuado em **parcela única;**

11.2. O pagamento, mediante a emissão de qualquer modalidade de ordem bancária, será realizado desde que a CONTRATADA efetue a cobrança de forma a permitir o cumprimento das exigências legais, principalmente no que se refere às retenções tributárias;

11.3. O Fiscal Administrativo do Contrato verificará a regularidade fiscal da CONTRATADA para com as Fazendas Federal, Estadual e Municipal do seu domicílio ou sede; da prova de regularidade relativa à Seguridade Social; do Certificado de Regularidade do FGTS – CRF, comprovando regularidade com o FGTS; e da Certidão Negativa de Débitos Trabalhistas – CNDT, emitida pela Justiça do Trabalho, bem como consulta ao CADIN;

11.3.1. A unidade responsável pelo pagamento poderá solicitar outros documentos que eximam o Tribunal Regional do Trabalho da 12ª Região das responsabilidades de ordem tributária, previdenciária ou trabalhista;

11.4. Se a Nota Fiscal for apresentada com erro, será devolvido para retificação e reapresentação, acrescentando-se no prazo fixado no caput os dias que se passarem entre a data da devolução e a reapresentação;

11.5. Observar-se-á ainda se o CNPJ apresentado na Nota Fiscal é o mesmo constante dos documentos habilitatórios;

11.6. Será efetuada pelo CONTRATANTE a retenção na fonte dos tributos e contribuições elencados na legislação em vigor, tais como, IR, CSLL, COFINS e PIS/PASEP;

11.7. A retenção dos tributos não será efetuada caso a CONTRATADA apresente junto a Nota Fiscal/Fatura a comprovação de que a mesma é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES;

11.8. As Notas Fiscais, para fins de liquidação e pagamento das despesas, deverá ser entregue exclusivamente ao Gestor do Contrato, através do endereço eletrônico seinfra@trt12.jus.br.

11.9. Não será efetuado qualquer pagamento à CONTRATADA enquanto houver pendência de liquidação da obrigação financeira em virtude de inadimplência contratual. Esse fato não será gerador de direito a reajustamento de preços ou atualização monetária;

11.10. O pagamento fica vinculado, ainda à comprovação do recolhimento do ISS referente aos bens/serviços, no que couber, junto ao órgão arrecadador do Município/Estado;

11.11. Em tratando-se de Nota Fiscal de serviços, caso a empresa seja optante pelo Simples Nacional, esta deverá conter a alíquota a recolher conforme o seu enquadramento;

11.12. Quando da ocorrência de eventuais atrasos de pagamentos provocados exclusivamente pela Administração do CONTRATANTE, o valor devido deverá ser acrescido

de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I = \frac{TX}{100}^{\frac{}{365}} \quad e \quad EM = I * N * VP$$

Onde**:**

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso.

CLÁUSULA DOZE – DA VIGÊNCIA

12.1. O Contrato terá vigência de **48 (quarenta e oito) meses**, contados a partir da data de sua assinatura, sem prejuízo das garantias contratuais previstas, na forma disposta no artigo 57, inciso IV, da Lei N° 8.666/1993.

CLÁUSULA TREZE – DA GARANTIA DE EXECUÇÃO DO CONTRATO

13.1. No prazo de 10 dias após a assinatura do contrato, a CONTRATADA prestará garantia no valor correspondente a 5% (cinco por cento) do valor total do Contrato, conforme o disposto no art. 56, § 1º, da Lei nº 8.666/93. Essa garantia poderá ser prestada em uma das seguintes modalidades:

13.1.1. Caução em dinheiro ou em títulos da dívida pública;

13.1.2. Fiança bancária;

13.1.3. Seguro garantia.

13.2. Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 15 (quinze) dias úteis, contados da data em que for notificada pelo Contratante;

13.3. A garantia somente será restituída à CONTRATADA após o integral cumprimento das obrigações contratuais;

13.4. Se a garantia a ser apresentada for em títulos da dívida pública, deverá ser emitida sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

13.5. A garantia prestada deverá ter vigência durante todo o período da contratação;

13.6. A não apresentação da garantia no prazo estipulado implicará as mesmas penalidades previstas para o atraso na entrega do objeto, podendo resultar inclusive na inexecução total do contrato.

CLÁUSULA QUATORZE – DAS PENALIDADES

14.1. Com fundamento no artigo 7º da Lei nº 10.520/2002, ficará impedida de licitar e contratar com a União e será descredenciada do SICAF, **pelo prazo de até 5 (cinco) anos**, garantida a ampla defesa, sem prejuízo da rescisão unilateral do contrato e da aplicação de **multa de até 15% (quinze por cento)** sobre o valor total da contratação, a CONTRATADA que:

14.1.1. Apresentar documentação falsa.
14.1.2. Fraudar a execução do contrato.
14.1.3. Comportar-se de modo inidôneo.
14.1.4. Cometer fraude fiscal, ou
14.1.5. Fizer declaração falsa.

14.2. Reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei nº 8.666/1993.

14.3. No caso de atraso no início da prestação dos serviços, garantida a ampla defesa e o contraditório, a CONTRATADA estará sujeita à aplicação de multa de até **0,25% por dia de atraso** incidente sobre o valor total do Contrato, que será aplicada a partir do 2º dia útil da inadimplência, contado da data definida para regular o cumprimento da obrigação até a data do efetivo adimplemento, observando o limite de **30 (trinta) dias**. Após esse prazo, será considerada a **inexecução total do contrato**, podendo ensejar a rescisão contratual, sem prejuízo ainda da cobrança de multa moratória eventualmente aplicada ou em fase de aplicação, sendo aplicadas cumulativamente.

14.4. Em consonância ao disposto no art. 2º da Lei nº 9784/1999 e suas alterações posteriores, as multas obedecerão ao princípio da proporcionalidade e ao atendimento do interesse público, desta forma serão definidos, níveis para as gravidades das infrações a serem aplicadas, conforme tabela abaixo:

Gravidade da Infração	Correspondência
1	Advertência por escrito
2	Multa de 0,50% sobre o valor do Contrato
3	Multa de 1,00% sobre o valor do Contrato
4	Multa de 2,50% sobre o valor do Contrato
5	Multa de 7,50% sobre o valor do Contrato

14.5. Nos casos de descumprimento de obrigação contratual, garantida a ampla defesa e o contraditório, a CONTRATADA estará sujeita à aplicação de multa conforme a tabela abaixo:

SANÇÕES GERAIS		
INFRAÇÃO	**GRAVIDADE**	
	Primeira Ocorrência	**Reincidência**
Não manter, durante a execução do Contrato, as condições de habilitação exigidas no instrumento convocatório para a contratação.	1	3
Entregar o Objeto **fora de conformidade** com as especificações constantes do Termo de Referência e demais	3	4

disposições contratuais.		
Não manter a proposta comercial na realização do certame.	5	N/A
Desacatar as orientações do Gestor do Contrato ou não prestar os esclarecimentos solicitados e atendimento das reclamações formuladas.	2	3
Deixar de observar as políticas de segurança e normas de acesso do CONTRATANTE.	4	5

SANÇÕES ESPECÍFICAS		
INFRAÇÃO	**GRAVIDADE**	
	Primeira Ocorrência	**Reincidência**
Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços contratuais.	4	5
Deixar de cumprir os prazos estabelecidos no subitem 15.4 do Termo de Referência do Edital do pregão 11/2021, que resultou na ARP 5/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante para o **nível 1** de impacto.	3	4
Deixar de cumprir os prazos estabelecidos no subitem 15.4 do Termo de Referência do Edital do pregão 11/2021, que resultou na ARP 5/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante para o **nível 2** de impacto.	2	3
Deixar de cumprir os prazos estabelecidos no subitem 15.4 do Termo de Referência do Edital do pregão 11/2021, que resultou na ARP 5/2021, ambos do TRT13, da qual o TRT da 12ª Região é participante para o **nível 3** de impacto.	1	2
Deixar de cumprir o cronograma de treinamento, a ser definido junto à CONTRATANTE	1	2

14.6. Será garantido o direito à prévia e ampla defesa, sem prejuízo das responsabilidades civil e criminal, ressalvados os casos devidamente justificados e acatados pelo CONTRATANTE.

14.7. Conforme o caso, poderão ser aplicadas as penalidades previstas no art. 87 da Lei nº 8.666/93 abaixo transcritas:

I – advertência;

II – multa, na forma prevista no instrumento convocatório ou no contrato;

III – suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos;

IV – declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Administração pelos prejuízos resultantes e após decorrido o prazo da sanção aplicada com base no inciso anterior.

14.8. As sanções previstas nos incisos I, III e IV da subcláusula 14.7. poderão ser aplicadas cumulativamente com a sanção prevista no inciso II da referida subcláusula, garantida a defesa prévia no prazo de 5 (cinco) dias úteis.

CLÁUSULA QUINZE – DA FISCALIZAÇÃO

15.1. O CONTRATANTE indicará servidor(es) para gestão e fiscalização do contrato, aqui denominados FISCALIZAÇÃO, responsáveis para acompanhar e fiscalizar o fornecimento dos produtos contratados, nos moldes delineados no Termo de Designação de Gestão e Fiscalização, conforme disposto no art. 67 da Lei nº 8.666, 21 de junho de 1993, e na Portaria nº 163/2020 de Gestão e Fiscalização da Execução dos Contratos Administrativos, no Guia para Gestão e Fiscalização de Contratos e no Manual de Fiscalização de Obras do TRT12.

15.2. O exercício da fiscalização pelo CONTRATANTE não excluirá ou reduzirá a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior.

15.3. A execução do contrato e a fiscalização será exercida por servidor ou comissão designado(s) pela administração que atuarão na forma da legislação pertinente e do Manual do Gestor de Contratos do CONTRATANTE.

CLÁUSULA DEZESSEIS – DA RESCISÃO

16.1. A inexecução total ou parcial do Contrato enseja sua rescisão, na forma do art. 77 da Lei n.º 8.666/93, constituindo motivo para rescisão aqueles previstos no art. 78 do mesmo diploma legal.

CLÁUSULA DEZESSETE – DA PUBLICAÇÃO

17.1. A publicação resumida deste Contrato na Imprensa Oficial, que é condição indispensável para sua eficácia, será providenciada pelo CONTRATANTE, nos termos do parágrafo único do artigo 61 da Lei n.º 8.666/93.

CLÁUSULA DEZOITO – DOS CASOS FORTUITOS, DE FORÇA MAIOR OU OMISSOS E DISPOSIÇÕES FINAIS

18.1. Tal como prescrito na lei, o CONTRATANTE e a CONTRATADA não serão responsabilizados por fatos comprovadamente decorrentes de casos fortuitos ou de força maior, ocorrências eventuais cuja solução se buscará mediante acordo entre as partes.

18.2. A Administração do Contratante analisará, julgará e decidirá, em cada caso, as questões alusivas a incidentes que se fundamentem em motivos de caso fortuito ou de força maior.

Parágrafo primeiro. Para os casos previstos no *caput* desta cláusula, o Contratante poderá atribuir a uma comissão designada a responsabilidade de apurar os atos e fatos comissivos ou omissivos que se fundamentem naqueles motivos.

Parágrafo segundo. As exceções aqui referenciadas serão sempre tratadas com máxima cautela, zelo profissional, senso de responsabilidade e ponderação, para que ato de mera e excepcional concessão do Contratante, cujo objetivo final é o de atender tão-somente ao interesse público, não seja interpretado como regra contratual.

Parágrafo terceiro. Para assegurar rápida solução às questões geradas em face da perfeita execução do presente contrato, fica desde já compelida a Contratada a avisar, por escrito e de imediato, qualquer alteração em seu endereço ou telefone.

Parágrafo quarto. Quaisquer tolerâncias entre as partes não importarão em novação de qualquer uma das cláusulas ou condições estatuídas neste contrato, as quais permanecerão íntegras.

Parágrafo quinto. Aos casos omissos não amparados pela legislação de direito público, pela lei que rege as contratações, pelos regulamentos e normas internas do Tribunal e da Justiça do Trabalho, aplicar-se-ão, supletivamente, o Código de Defesa do Consumidor, os princípios da teoria geral dos contratos e as disposições do direito privado.

CLÁUSULA DEZENOVE – DO FORO

19.1. Fica eleito o foro da Justiça Federal, Seção Judiciária de Santa Catarina, na Cidade de Florianópolis, para dirimir qualquer litígio oriundo do presente Contrato, que não puderem ser administrativamente solucionados, renunciando-se a qualquer outro por mais privilegiado que seja.

E, para firmeza e validade do que foi pactuado, firmou-se o presente termo de contrato, o qual, depois de lido, é assinado eletrônica/digitalmente pelos representantes das partes, considerando-se efetivamente formalizado a partir da data da última assinatura.

TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO
Maria de Lourdes Leiria
Desembargadora do Trabalho-Presidente

ISH TECNOLOGIA S/A
Hélio Ferreira da Silva Júnior
Representante Legal

ANEXO I

ESPECIFICAÇÕES COMPLETAS REFERENTES A SOLUÇÃO DE SOFTWARE DE SEGURANÇA (ANTIVÍRUS) PARA ENDPOINTS (ESTAÇÕES DE TRABALHO, DISPOSITIVOS MÓVEIS E SERVIDORES FÍSICOS, INCLUINDO CAPACITAÇÃO E INSTALAÇÃO

A solução de software de segurança e os serviços oferecidos devem atender aos seguintes requisitos técnicos:

A.1. Requisitos Gerais – Comuns aos itens 1 e 2

A.1.1. O console de gerenciamento deve estar disponível para instalação On-Premise ou utilização em nuvem (cloud do fabricante).

A.1.1.1. Para o caso de appliance virtual, deverá suportar no mínimo o Hypervisor VMWare vSphere 6.7 ou superior;

A.1.1.2. Para o caso de instalação em sistema operacional Windows, deverá ser compatível, no mínimo, com a versão Microsoft Windows Server 2016 ou superior.

A.1.2. A solução deve possuir console de gerenciamento centralizado com acesso via WEB (HTTPS) ou MMC (Microsoft Management Console);

A.1.3. O Console de Gerenciamento deve conter:

A.1.3.1. Painel para monitoramento;
A.1.3.2. Capacidade de criação de relatórios;
A.1.3.3. Mecanismo para envio de notificações administrativas (e-mail);

A.1.4. Deve permitir inventário das máquinas gerenciadas pela solução;

A.1.5. O console central deve mostrar quantos dispositivos estão sendo gerenciados e quais seus sistemas operacionais;

A.1.6. Deve possuir a capacidade de autenticação dos usuários do console de gerenciamento através do Microsoft Active Directory.

A.1.6.1. Deve permitir a definição de perfis com diferentes níveis de privilégios de administração da solução, baseados em usuários ou grupos do Microsoft Active Directory;

A.1.6.2. Capacidade de exportar relatórios para, no mínimo 2, dos seguintes tipos de arquivos: PDF, HTML e CSV;
A.1.6.3. Capacidade de enviar e-mails para contas específicas, em caso de algum evento;

A.1.6.4. O console de gerenciamento deve fornecer as seguintes informações dos computadores protegidos:

A.1.6.4.1. Horário da última conexão da máquina com o servidor administrativo ou, no mínimo, o tempo decorrido desde a última conexão;

A.1.6.4.2. Data e horário da última verificação executada na máquina;

A.1.6.4.3. Se a solução está instalado;

A.1.6.4.4. Versão do antivírus instalado na máquina gerenciada;

A.1.6.4.5. Se o antivírus está atualizado;

A.1.6.4.6. Nome do computador;

A.1.6.4.7. Domínio ou grupo de trabalho do computador;

A.1.6.4.8. Sistema operacional e Service Pack/Build;

A.1.6.4.9. Endereço IP.

A.1.7. Capacidade de instalar remotamente a solução nas estações (endpoints) e servidores Windows, através de compartilhamento administrativo, login script ou GPO do Microsoft Active Directory, no mínimo;

A.1.8. Capacidade de gerar pacotes auto-executáveis para a instalação do software para gerenciamento, além de automatização para instalação de todos os módulos e informações necessárias para o funcionamento do produto (licenças, configurações, etc);

A.1.9. Capacidade de importar a estrutura do Microsoft Active Directory para a descoberta de máquinas da rede corporativa;

A.1.10. Capacidade de monitorar a rede, em diferentes sub redes, a fim de encontrar máquinas novas, para a instalação automática da solução de segurança;

A.1.11. Deve ser capaz de eleger qualquer computador cliente ou servidor como repositório de vacinas e de pacotes de instalação, sem a necessidade de instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar o tráfego da rede;

A.1.12. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar o tráfego de link entre sites diferentes;

A.1.13. Deve permitir a herança de tarefas e políticas na estrutura de hierarquia de servidores administrativos;

A.1.14. Capacidade de realizar atualização incremental de vacinas nos computadores clientes a partir da rede local e da Internet;

A.1.15. A atualização incremental de vacinas deve ser disponibilizada, no mínimo, com frequência diária;

A.1.16. A solução deve possuir integração com o Active Directory, de maneira a permitir a definição de políticas diferentes, baseadas em usuários ou grupos;

A.1.17. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

A.1.18. Deve armazenar histórico das alterações feitas em políticas;

A.1.19. Deve permitir a realocação de máquinas novas na rede para um determinado grupo utilizando os seguintes parâmetros:

A.1.19.1. Nome do computador;

A.1.19.2. Range de IP;

A.1.19.3. Sistema Operacional;

A.1.20. Caso a solução ofertada não atenda na totalidade os itens aqui referidos, será permitido a composição com outras soluções a fim de atender na plenitude dos itens aqui descritos;

A.1.21. Deve possuir uma base de inteligência global, do próprio fabricante, sobre campanhas de ameaças existentes;

A.1.22. Deve ser capaz de dar visibilidade sobre campanhas de ameaças globais;

A.1.23. A solução deve ser capaz de proporcionar a busca por ameaças baseadas em IOCs;

A.1.24. Deve ser capaz de indicar quantos e quais dispositivos dentro da empresa estão vulneráveis a determinada ameaça;

A.1.25. Deve ser capaz de mostrar o nível de postura de segurança da organização, em relação às políticas aplicadas no ambiente protegido.

A.1.26. Cada ameaça identificada pela solução deverá possuir as seguintes informações:

A.1.26.1. Detalhes do ataque;

A.1.26.2. IOCs;

A.1.26.3. Detalhes do Impacto no ambiente;

A.1.26.4. Endpoints afetados;

A.1.26.5. Comportamento da ameaça.

A.2. Item 1 – Licença de software de segurança para estações de trabalho e servidores.

A.2.1. Requisitos Gerais

A.2.1.1. Prover segurança para as estações de trabalho (endpoints), sejam físicas ou em ambiente virtualizado;

A.2.1.2. Se comunicar com console central de gerenciamento, de forma que seja possível gerenciar todas as funcionalidades;

A.2.1.3. Detectar e eliminar programas maliciosos (malwares), tais como vírus, ransomware, spywares, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

A.2.1.4. Identificar e proteger contra eventuais vulnerabilidades dos sistemas operacionais e aplicações;

A.2.1.5. Deve detectar e eliminar programas maliciosos em:

A.2.1.5.1. Processos Em Execução Em Memória principal (RAM);

A.2.1.5.2. Arquivos Executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

A.2.1.5.3. Arquivos Compactados, em tempo real ou no ato de sua execução, com os seguintes formatos: ZIP, EXE, ARJ, RAR, e CAB;

A.2.1.5.4. Detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex.

A.2.1.6. Capacidade de detecção heurística de malwares desconhecidos;

A.2.1.7. Possuir tecnologia de Machine Learning de pre-execution, run time machine e post-execution;

A.2.1.8. Deve prover, no mínimo, as seguintes proteções:

A.2.1.8.1. Antivírus de arquivos;

A.2.1.8.2. Antivírus web (verificação de sites e downloads contra malwares);

A.2.1.8.3. Firewall de host com HIPS (Host Intrusion Prevention System) e/ou HIDS (Host Intrusion Detection System);

A.2.1.8.4. Proteção contra ataques aos serviços/processos do antivírus;

A.2.1.8.5. Controle de dispositivos;

A.2.1.8.6. Controle de execução de aplicativos;

A.2.1.8.7. Controle de acesso a sites por categorias (Adulto, Jogos, etc);

A.2.1.8.8. Prevenção contra exploração de vulnerabilidades.

A.2.1.8.9. Capacidade de integração com a Antimalware Scan Interface (AMSI).

A.2.1.9. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

A.2.2. Detalhamento das proteções:

A.2.2.1. Antivírus de arquivos:

A.2.2.1.1. Verificar todos os arquivos criados, acessados ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;

A.2.2.1.2. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

A.2.2.1.3. Deve possuir Módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

A.2.2.1.4. Deve possuir Módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro;

A.2.2.1.5. Capacidade para definir escopo de varredura / rastreamento: todos os discos locais, discos específicos;

A.2.2.1.6. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí-los da verificação;

A.2.2.1.7. Possibilidade de definir frequência de varredura;

A.2.2.1.8. Capacidade de realizar a verificação “inteligente” de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá-la apenas a partir da extensão do arquivo;

A.2.2.1.9. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

A.2.2.2. Antivírus web:

A.2.2.2.1. O antivírus web deve ter a capacidade de verificação de tráfego HTTP/HTTPS e scripts (JavaScript, Visual Basic Script, etc.);

A.2.2.2.2. Capacidade de limitar o acesso a sites da internet por reputação;

A.2.2.2.3. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus web;

A.2.2.2.4. Capacidade de verificar tráfego nos browsers: Internet Explorer, Mozilla Firefox e Google Chrome.

A.2.2.3. Firewall de host com HIPS e/ou HIDS

A.2.2.3.1. O módulo de firewall deve conter, no mínimo, dois conjuntos de regras:

A.2.2.3.1.1. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas ou, definir o comportamento da filtragem de pacotes, podendo definir pelo menos, mas não limitado a: permitir, bloquear ou bloquear com exceções aos pacotes de rede;

A.2.2.3.1.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo terá acesso à rede.

A.2.2.3.2. Deve possuir módulo HIPS e/ou HIDS para proteção/detecção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

A.2.2.4. Proteção contra Ameaças Avançadas

A.2.2.4.1. A solução deve permitir a análise comportamental avançada de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware);

A.2.2.4.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas permitindo sua execução e analisando seu comportamento no endpoint;

A.2.2.4.3. Deve permitir criar exceções para aplicações confiáveis, evitando que sejam bloqueadas por componentes de detecção;

A.2.2.4.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;

A.2.2.4.5. Solução deve manter um cache de reputação local com informações de aplicações conhecidas, desconhecidas e maliciosas;

A.2.2.4.6. Dentre os comportamentos maliciosos, deve ser capaz de “bloquear” ou “detectar e trazer rastreabilidade sobre”:

A.2.2.4.6.1. Acesso local a partir de cookies;

A.2.2.4.6.2. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;

A.2.2.4.6.3. Criação de threads em outro processo;

A.2.2.4.6.4. Desativação de executáveis críticos do sistema operacional;

A.2.2.4.6.5. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;

A.2.2.4.6.6. Gravação e Leitura na memória de outro processo;

A.2.2.4.6.7. Modificação da política de firewall do Windows;

A.2.2.4.6.8. Modificação da pasta de tarefas do Windows;

A.2.2.4.6.9. Modificação de arquivos críticos do Windows e Locais do Registro;

A.2.2.4.6.10. Modificação de arquivos executáveis portáteis;

A.2.2.4.6.11. Modificação de bit de atributo oculto;

A.2.2.4.6.12. Modificação de bit de atributo somente leitura;

A.2.2.4.6.13. Modificação de entradas de registro de DLL AppInit;

A.2.2.4.6.14. Modificação de locais do registro de inicialização;

A.2.2.4.6.15. Modificação de pastas de dados de usuários;

A.2.2.4.6.16. Modificação do local do Registro de Serviços;

A.2.2.4.6.17. Suspensão de um processo;

A.2.2.4.7. Deve ser capaz de bloquear ou apenas informar quando uma ameaça for encontrada;

A.2.2.4.8. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem;

A.2.2.4.9. Deve possuir modo de ativação da análise comportamental avançada para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

A.2.2.4.10. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;

A.2.2.4.11. 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;

A.2.2.4.12. Utilizar técnicas de machine learning para detecção de ameaças

A.2.2.5. Controle de dispositivos:

A.2.2.5.1. Deve possuir módulo de controle de dispositivos, que permita o bloqueio e a ativação de dispositivos;

A.2.2.5.2. Capacidade de liberar o acesso a um dispositivo específico sem a necessidade de desabilitar a proteção ou da intervenção local na máquina do usuário;

A.2.2.5.3. Capacidade de adicionar novos dispositivos por Class ID/Hardware ID.

A.2.2.6. Controle de execução de aplicativos:

A.2.2.6.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política;

A.2.2.6.2. Deve ser capaz de realizar um inventário das estações de trabalho protegidas informando todos os executáveis presentes;

A.2.2.6.3. Como resultado do inventário, a solução deve armazenar o nome completo do arquivo, tamanho, checksum, tipo de arquivo, nome da aplicação;

A.2.2.6.4. Ao detectar um executável, a solução deverá consultar a Solução de reputação de arquivos e compartilhamento de informações de segurança;

A.2.2.6.5. Caso não seja possível efetuar comunicação com a Solução de reputação de arquivos e compartilhamento de informações de segurança, o módulo deve
realizar consulta de reputação para o Centro de Inteligência do fabricante;

A.2.2.6.6. Deve ser possível criar uma imagem base para a criação de uma política geral;

A.2.2.6.7. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;

A.2.2.6.8. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA- 1).

A.2.2.6.9. A solução deve suportar as seguintes modalidades de proteção:

A.2.2.6.9.1. Criação de uma lista de aplicações autorizadas que podem ser executadas, onde todas as demais aplicações são impedidas de serem executadas;

A.2.2.6.9.2. Criação de uma lista de aplicações não autorizadas que não podem ser executadas;

A.2.2.6.9.3. 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.

A.2.2.6.10. Deve ser capaz de proteger em modo standalone - online ou offline;

A.2.2.6.11. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize-as de forma a adaptar a necessidade do órgão;

A.2.2.6.12. Permitir o bloqueio de aplicações e os processos que a aplicação interage;

A.2.2.6.13. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;

A.2.2.6.14. Permitir monitoração de Hooking de aplicações;

A.2.2.7. Proteção contra ransomwares:

A.2.2.7.1. Bloquear a criptografia de arquivos em recursos compartilhados a partir de um processo malicioso, inclusive, que esteja sendo executado em outra máquina;

A.2.2.7.2. Monitoramento de pastas compartilhadas no ambiente Windows, rastreando o estado dos arquivos armazenados e os protegendo;

A.2.2.7.3. Na detecção de atividade maliciosa de criptografia por ransomware, o antivírus deve interromper o processo de criptografia e restaurar os arquivos ao seu estado original, impedindo a perda de dados corporativos.

A.2.3. Características do módulo de reputação de arquivos e compartilhamento de informações de segurança:

A.2.3.1. Deve ser fornecida em formato de appliance virtual ou existir nativamente no gerenciamento do produto, sem a necessidade de appliance;

A.2.3.2. Se for entregue no formato de appliance virtual, deve ser compatível no mínimo com ambiente virtualizado VMWare ESXi;

A.2.3.3. A solução deve possuir capacidade de criar uma reputação local ou utilizar uma já existente em nuvem através da catalogação de todos os executáveis existentes no ambiente;

A.2.3.4. O servidor de reputação deverá habilitar a troca de informação de ameaças entre os endpoints e servidores protegidos;

A.2.3.5. A troca de informação de ameaças deve se dar por meio de protocolo performático ou através da console de gerenciamento de forma criptografada;

A.2.3.6. De forma a permitir menor impacto na rede, para tal método de consulta dos clientes à base de dados poderá ser síncrona ou assíncrona;

A.2.3.7. A solução deverá apresentar a reputação dos arquivos definida para cada um dos ativos conectados, dentre eles:

A.2.3.7.1. Reputação local;

A.2.3.7.2. Reputação do centro de inteligência.

A.2.3.8. Após análise pela solução o administrador deve ter a possibilidade de:

A.2.3.8.1. Rastrear em quais estações o arquivo foi executado;

A.2.3.8.2. Identificar o arquivo como confiável;

A.2.3.8.3. Identificar o arquivo como desconhecido;

A.2.3.8.4. Identificar o arquivo como malicioso;

A.2.3.8.5. Analisar o certificado associado ao arquivo;

A.2.3.8.6. Identificar o certificado associado como confiável ou malicioso.

A.2.3.9. Deve ser possível bloquear a execução de arquivos suspeitos no ambiente e informar o usuário por meio de mensagem;

A.2.3.10. Deve ser capaz de identificar manualmente um arquivo e proibir que ele seja executado no ambiente.

A.2.4. Módulo de proteção para dispositivos móveis:

A.2.4.1. A solução de "Proteção para dispositivos móveis", deve proteger a CONTRATANTE contra as ameaças em dispositivos móveis, Android e iOS, incluindo malwares, ameaças de rede e defesa física dos dispositivos. O objetivo principal desta solução é proteger os usuários móveis, impedindo que ameaças nestes dispositivos possam impactar nos serviços e na rede da CONTRATANTE;

A.2.4.2. Características Gerais:

A.2.4.2.1. Deverá ser ofertado como um serviço on-premises (local) ou em console baseado em nuvem de forma a garantir suas funcionalidades independente da rede que o dispositivo estiver conectado;

A.2.4.2.2. A solução deverá possuir console WEB para administração da solução;

A.2.4.2.3. Possuir dashboard com os principais indicadores da solução, como Distribuição de níveis de risco, dispositivos em não conformidade, total de dispositivos protegidos e incidentes recentes;

A.2.4.2.4. Apresentar, nos dashboards, uma visão geral dos riscos examinados nos dispositivos móveis, como ameaças de rede e malwares encontrados;

A.2.4.2.5. Deverá possuir uma apresentação gráfica referente às informações dos dispositivos registrados na solução;

A.2.4.2.6. O console deverá apresentar os principais incidentes gerados, contendo todos os detalhes sobre o incidente e o dispositivo que o gerou;

A.2.4.2.7. Deverá ser compatível com os sistemas operacionais iOS e Android;

A.2.4.2.8. O cliente da solução deverá estar disponível nas lojas oficiais dos fabricantes, sendo Apple Store para iOS e Play Store para Android ou ser

instalado de forma remota através da console de gerenciamento.

A.2.4.2.9. Permitir configuração no cliente instalado nos dispositivos móveis para que nenhuma informação e alerta seja visível para o usuário final, através de modo não interativo;

A.2.4.2.10. Deverá possuir as seguintes características mínimas de proteção:

A.2.4.2.10.1. Proteção contra Malwares:

A.2.4.2.10.1.1. Proteção em tempo real contra malwares conhecidos e desconhecidos;

A.2.4.2.10.2. Defesa física

A.2.4.2.10.2.1. Identificação de upgrades do sistema operacional;

A.2.4.2.10.2.2. Identificação de dispositivo com root.

A.2.4.2.11. Deverá possuir integração com solução de SIEM de mercado;

A.2.4.2.12. A solução deve apresentar notificações de violações para o usuário final e para os administradores da solução, através de e-mail e notificações Push;

A.2.5. Compatibilidade

A.2.5.1. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações de trabalho:

A.2.5.1.1. Microsoft Windows 8 (e suas edições);

A.2.5.1.2. Microsoft Windows 8.1 (e suas edições);

A.2.5.1.3. Microsoft Windows 10 (e suas edições);

A.2.5.1.4. Ser compatível para instalação em sistemas legados em Windows 7.

A.2.5.2. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para servidores:

A.2.5.2.1. Microsoft Windows Server 2012 (e suas edições);

A.2.5.2.2. Microsoft Windows Server 2012 R2 (e suas edições);

A.2.5.2.3. Microsoft Windows Server 2016 (e suas edições);

A.2.5.2.4. Microsoft Windows Server 2019 (e suas edições).

A.2.5.3. A solução deve ser compatível para a funcionalidade de antimalware, no mínimo, com a seguinte distribuição/versão de sistema operacional Linux para

estações de trabalho e servidores:

A.2.5.3.1. Red Hat Enterprise 7.x e superior, 32 e 64 bits;

A.2.5.3.2. SUSE Linux Enterprise Server 12.x e superior, 32 e 64bits;

A.2.5.3.3. Ubuntu 16.04 e superior, 32 e 64bits;

A.2.5.3.4. CentOS 7.x e superior, 32 e 64bits;

A.2.5.3.5. Oracle Linux 7.x e superior, 32 e 64bits;

A.3. Item 2 – Licença de software para ambientes virtualizados.

A.3.1. Requisitos Gerais

A.3.1.1. Ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes VMware ESXi e Hyper-V;

A.3.1.2. Deve prover, no mínimo, as seguintes proteções:

A.3.1.2.1. Antivírus de arquivos que verifique todos os arquivos criados, acessados ou modificados;

A.3.1.2.2. Proteção contra ataques aos serviços/processos do antivírus.

A.3.1.3. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na remota;

A.3.1.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

A.3.1.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

A.3.1.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

A.3.1.4.3. Leitura de configurações;

A.3.1.4.4. Modificação de configurações.

A.3.1.5. Em caso de erros, deve ter a capacidade de criar logs e traces automaticamente, sem necessidade de uso de outros softwares;

A.3.1.6. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí-los da verificação;

A.3.1.7. Capacidade de realizar a verificação inteligente de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não a tomar apenas a partir da extensão do arquivo;

A.3.1.8. Capacidade de verificar objetos usando heurística;

A.3.1.9. Antes de qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

A.3.2. Compatibilidade

A.3.2.1. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações servidoras:

A.3.2.1.1. Microsoft Windows Server 2012 (e suas edições);

A.3.2.1.2. Microsoft Windows Server 2012 R2 (e suas edições);

A.3.2.1.3. Microsoft Windows Server 2016 (e suas edições);

A.3.2.1.4. Microsoft Windows Server 2019 (e suas edições).

A.3.2.2. A solução deve ser compatível, no mínimo, com as seguintes distribuições / versões de sistemas operacionais Linux para servidores:

A.3.2.2.1. RedHat Enterprise Linux 7.x e superior, 32 e 64bits;

A.3.2.2.2. SUSE Linux Enterprise Server 12 SP1 e superior, 32 e 64bits;

A.3.2.2.3. Ubuntu 16.04 LTS e superior, 32 e 64bits;

A.3.2.2.4. CentOS 7.x e superior, 32 e 64bits;

A.3.2.2.5. Oracle Linux 7.x e superior, 32 e 64bits;

A.4. Item 3 - Serviço de implantação e migração da solução para proteção de endpoints e servidores

A.4.1. A LICITANTE vencedora será inteiramente responsável pela instalação, atualização ou migração da solução antivírus atualmente em uso pela CONTRATANTE, bem como às despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

A.4.2. A instalação, atualização ou migração dos softwares em estações de trabalho poderá ser realizada remotamente, sem causar indisponibilidade do ambiente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

A.4.3. A instalação, atualização ou migração dos softwares em servidores de rede poderá ser realizada remotamente, devendo ser realizada em horários a serem definidos pela CONTRATANTE;

A.4.4. A CONTRATANTE poderá autorizar a instalação, atualização ou migração durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção;

A.4.5. O processo de instalação, atualização ou migração da solução deverá ser acompanhado por servidores da CONTRATANTE;

A.4.6. Para garantir que a instalação, atualização ou migração não afetará o ambiente da CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante;

A.4.7. Em caso de migração de solução, a CONTRATADA deverá:

A.4.7.1. Realizar a migração de todas políticas, regras e customizações configuradas no CONTRATANTE;

A.4.7.2. A CONTRATADA deverá se reunir com a equipe técnica da CONTRATANTE e elaborar um plano de migração, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço de migração;

A.4.7.3. A Migração da solução deverá seguir todos os procedimentos internos da CONTRATANTE, incluindo os processos de registro de mudanças, liberações e incidentes.

A.5. Item 4 - Treinamento e Atualização Tecnológica

A.5.1. A CONTRATADA deverá fornecer treinamento com carga horária mínima de 20 (vinte) horas, contemplando a perfeita instalação, operação, manuseio, gerenciamento, configuração e utilização das soluções contratadas;

A.5.2. Os treinamentos deverão ser realizados em dias úteis, em horário comercial;

A.5.3. O treinamento deverá ser realizado de forma remota;

A.5.4. Deverá ser disponibilizado material didático impresso e/ou em mídia, sem custo adicional para a CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), sendo aceitável o idioma inglês;

A.5.5. Deverá ser emitido certificado de participação ao final do curso a cada participante;

A.5.6. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato;

A.5.7. Caso o treinamento/atualização fornecido não for satisfatório, mediante avaliação tempestiva e fundamentada, tanto em relação à qualidade ou à carga horária efetiva, a CONTRATADA deverá realizá-los novamente, sem ônus adicional à CONTRATANTE;

A.5.8. A critério da CONTRATANTE, o treinamento poderá ser dividido em turmas;

A.5.9. O conteúdo programático deverá englobar, pelo menos, os seguintes assuntos:

A.5.9.1. Instalação do ambiente;

A.5.9.2. Manutenção básica, intermediária e avançada;

A.5.9.3. Configurações básicas e avançadas;

A.5.9.4. Verificação de alertas e erros;

A.5.9.5. Monitoramento e relatórios.

A.6. CONDIÇÕES DE FORNECIMENTO

A.6.1. Para comprovação das características mínimas relativas ao presente Termo de Referência, a proposta deverá vir acompanhada de manuais técnicos, catálogos técnicos, carta/declaração do fabricante ou publicações originais do fabricante, fazendo constar no documento técnico a identificação e página do documento onde se encontra descrita cada uma das características ofertadas.

A.6.1.1. Os documentos técnicos deverão ser apresentados junto com a proposta, por planilha contendo item, a descrição do item, e a comprovação técnica (de acordo com o item anterior).

A.6.1.2. As especificações das características técnicas da solução de segurança ofertada deverão estar descritas de forma clara e detalhada.

A.6.1.3. Será permitido o uso de expressões técnicas de uso comum na língua inglesa.

A.6.2. O TRT12, a seu exclusivo critério, poderá solicitar amostra da solução completa ofertada pelo licitante vencedor para realização de testes que venham demonstrar a efetiva conformidade com a especificação técnica constante deste Termo de Referência.

A.6.2.1. A adjudicação da solução vencedora dependerá da aprovação dos testes de funcionalidade da solução de segurança, a serem realizados na demonstração.