REPÚBLICA FEDERATIVA DO BRASIL
PODER JUDICIÁRIO

FRANCISCO JONATHAN REBOUCAS MAIA

MALOTE DIGITAL

Tipo de documento: Administrativo
Código de rastreabilidade: 513202117674163
Nome original: TR - Antivírus.pdf
Data: 05/05/2021 11:31:58
Remetente:
Paulo
Secretaria de Tecnologia da Informação e Comunicação
Tribunal Regional do Trabalho da 13ª Região
Prioridade: Normal.
Motivo de envio: Para conhecimento.
Assunto: Solicita concordância com ETP e TR Segurança de Endpoints (Antivírus)

1. OBJETO

Registro de preço para aquisição de Solução de Segurança de Endpoints.

A aquisição visa atender as necessidades deste Regional e dos participantes deste processo de contratação listados abaixo:

- Tribunal Regional do Trabalho da 1ª Região - CNPJ: 02.578.421/0001-20;
- Tribunal Regional do Trabalho da 2ª Região - CNPJ: 03.241.738/0001-39;
- Tribunal Regional do Trabalho da 3ª Região - CNPJ: 01.298.583/0001-41;
- Tribunal Regional do Trabalho da 4ª Região - CNPJ: 02.520.619/0001-52;
- Tribunal Regional do Trabalho da 5ª Região - CNPJ: 02.839.639/0001-90;
- Tribunal Regional do Trabalho da 6ª Região - CNPJ: 02.566.224/0001-90;
- Tribunal Regional do Trabalho da 7ª Região - CNPJ: 03.235.270/0001-70;
- Tribunal Regional do Trabalho da 8ª Região - CNPJ: 01.547.343/0001-33;
- Tribunal Regional do Trabalho da 9ª Região - CNPJ: 03.141.166/0001-16;
- Tribunal Regional do Trabalho da 10ª Região - CNPJ: 02.011.574/0001-90;
- Tribunal Regional do Trabalho da 11ª Região - CNPJ: 01.671.187/0001-18;
- Tribunal Regional do Trabalho da 12ª Região - CNPJ: 02.482.005/0001-23;
- Tribunal Regional do Trabalho da 14ª Região - CNPJ: 03.326.815/0001-53;
- Tribunal Regional do Trabalho da 15ª Região - CNPJ: 03.773.524/0001-03;
- Tribunal Regional do Trabalho da 16ª Região - CNPJ: 23.608.631/0001-93;
- Tribunal Regional do Trabalho da 17ª Região - CNPJ: 02.488.507/0001-61;
- Tribunal Regional do Trabalho da 18ª Região - CNPJ: 02.395.868/0001-63;
- Tribunal Regional do Trabalho da 19ª Região - CNPJ: 35.734.318/0001-80;
- Tribunal Regional do Trabalho da 20ª Região - CNPJ: 01.445.033/0001-08;
- Tribunal Regional do Trabalho da 21ª Região - CNPJ: 02.544.593/0001-82;
- Tribunal Regional do Trabalho da 22ª Região - CNPJ: 03.458.141/0001-40;
- Tribunal Regional do Trabalho da 23ª Região - CNPJ: 37.115.425/0001-56;
- Tribunal Regional do Trabalho da 24ª Região - CNPJ: 37.115.409/0001-63;
- Tribunal Superior do Trabalho - CNPJ: 00.509.968/0001-48;

2. MOTIVAÇÃO DA CONTRATAÇÃO

A utilização de Solução de Segurança de Endpoints possibilita a redução dos riscos de fraude, vazamento de informações, inconsistência de informações, indisponibilidade das aplicações corporativas e, até mesmo, sabotagens que podem gerar falso repúdio.

A solução de segurança de endpoints atualmente em uso na Justiça do Trabalho foi adquirida por meio da Ata de Registro de Preços 01/2017. A contratação nacional foi feita em 2017 pelo TRT 13. A solução vem atendendo bem às necessidades do regional, e em 2021 se encerrará o contrato atual de suporte e atualização. Dessa forma, será necessária uma nova aquisição. Situação análoga acontece nos demais regionais. Diante do exposto, a contratação em tela se faz

necessária como forma de contribuir para a segurança das informações estratégicas e para a continuidade dos serviços prestados pela Justiça do Trabalho. É irrefutável a necessidade de proteção de quaisquer equipamentos conectados à rede de dados da Justiça do Trabalho contra códigos maliciosos que possam colocar em risco os dados contidos, não só no equipamento originário, mas também nos demais equipamentos conectados à rede corporativa. A solução de segurança de endpoints é uma parte fundamental dentro de um conjunto de ações que visam à segurança das informações corporativas da Justiça do Trabalho.

O Conselho Superior da Justiça do Trabalho tem adotado modelo de descentralização da aquisição de bens e contratação de serviços na área de Tecnologia da Informação e Comunicação, em conformidade com o Ato n.º 133/2009. Como parte do processo de integração e padronização dos sistemas informatizados dos órgãos da Justiça do Trabalho – conduzido pelo CSJT e pelo TST, com apoio e participação dos TRTs – adota-se, sempre que possível, uma política de "compras centralizadas" na aquisição de bens comuns de informática e na contratação de serviços comuns da tecnologia da informação, capazes de atender às necessidades gerais. Tal política tem proporcionado ampla economia de recursos financeiros, especialmente em comparação com o método de compras regionalizadas. Diante desse cenário, o Comitê Gestor de Tecnologia da Informação e das Comunicações da Justiça do Trabalho – CGTIC-JT, propôs que alguns dos Tribunais Regionais conduzissem os procedimentos licitatórios para aquisições e contratações com vistas ao atendimento das demandas da Justiça do Trabalho.

O Tribunal Regional do Trabalho da 13ª Região foi designado como órgão gerenciador da licitação relativa à solução de segurança de endpoints e efetuará o controle e administração do Registro de Preços.

3. OBJETIVOS A SEREM ALCANÇADOS

- **Objetivo Geral:** Contribuir para a segurança da informação no ambiente computacional da Justiça do Trabalho.
- **Objetivo Específico:** Manter os endpoints protegidos da ação de softwares maliciosos.

4. BENEFÍCIOS DIRETOS E INDIRETOS

- Redução dos riscos de segurança associados à Tecnologia da Informação;
- Redução da quantidade de incidentes de segurança relacionados a ameaças oriundas de malwares;
- Otimização do uso dos recursos de Tecnologia da Informação;
- Proteção das estações e servidores contra ameaças eletrônicas tais como vírus, *worms*, *trojans*, *spywares*, *ransomwares*, entre outras;
- Suporte técnico especializado prestado pelo fabricante do produto;
- Solução de segurança de endpoints atualizada e com uso das tecnologias mais atualizadas;
- Ganho de produtividade com a não parada de equipamentos por problemas com infecção de códigos maliciosos;
- Redução de risco relacionado a vazamento de informações.

5. ALINHAMENTO ESTRATÉGICO

A contratação está em consonância com:

- **Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) 2015-2020**, conforme Objetivo 8: Aprimorar a segurança da informação;
- **Planejamento Estratégico da Justiça do Trabalho 2015-2020**, conforme Objetivo: Aprimorar a infraestrutura e a governança de TIC;
- **Planejamento Estratégico de TIC da Justiça do Trabalho (PETIC-JT) 2015-2020**, conforme objetivo "Garantir a infraestrutura de TIC que suporte o negócio";
- **Planejamento Estratégico Institucional (PEI) TRT13 2015-2020**, conforme Objetivo Estratégico 7: Garantir a infraestrutura e a governança de TIC;

6. ESTUDOS PRELIMINARES

Em atendimento à Resolução CNJ nº 182, de 17 de outubro de 2013, os estudos técnicos preliminares sobre a presente aquisição foram realizados e podem ser consultados no protocolo administrativo 000-3769/2020;

7. RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE CADA ITEM

- Foram consultados os núcleos de Apoio ao Usuário e Infraestrutura para que fosse feito o levantamento da quantidade de **endpoints (estações de trabalho, dispositivos móveis e servidores físicos e virtuais)** a serem protegidos, chegando ao quantitativo listado na tabela abaixo. Foram indicados, ainda, 03 (três) servidores de cada núcleo para realizarem o treinamento:
- Foi realizada uma consulta prévia aos Tribunais Regionais do Trabalho para saber a demanda de cada um[1]. A seguir, apresentamos o resultado desse levantamento:

Órgão	UF	Quantidade para aquisição imediata			
		Item 1 - Licença de software de segurança para endpoints (estações de trabalho, dispositivos móveis e servidores físicos) (nº de licenças)	**Item 2 - Licença de software de segurança para ambiente virtualizado (nº de licenças)**	**Item 3 - Implantação e configuração da solução + Repasse de conhecimento hands-on (serviço)**	**Item 4 - Treinamento EAD de capacitação técnica para administração da solução (nº de alunos)**
TRT1	RJ	6.556	200	1	4
TRT2	SP	3.900	0	1	8
TRT3	MG	0	0	1	0
TRT4	RS	0	0	0	0
TRT5	BA	3.500	70	1	5
TRT6	PE	2.900	250	0	0
TRT7	CE	1.850	0	1	3
TRT8	PA/AP	2.850	150	1	5

[1] Vide Ofício 03/2021, enviado no dia 26/01/2021 e constante nos autos do processo.

TRT9	PR	4.763	100	1	3
TRT10	DF/TO	1.800	0	1	2
TRT11	AM/RR	1.520	350	1	6
TRT12	SC	2.560	10	1	8
TRT13	PB	1.700	300	1	6
TRT14	RO/AC	1.250	200	1	3
TRT15	SP	5.500	0	1	6
TRT16	MA	0	0	0	0
TRT17	ES	1.300	0	1	7
TRT18	GO	1.900	200	1	2
TRT19	AL	0	0	0	0
TRT20	SE	800	100	1	4
TRT21	RN	1.400	200	1	3
TRT22	PI	700	300	1	6
TRT23	MT	1.000	80	1	1
TRT24	MS	1.300	70	1	5
TST	DF	3.776	0	1	4
Total		52.825	2.580	21	91

Órgão	**UF**	**Quantidade máxima para registro**			
		Item 1 - Licença de software de segurança para endpoints (estações de trabalho, dispositivos móveis e servidores físicos) (nº de licenças)	**Item 2 - Licença de software de segurança para ambiente virtualizado (nº de licenças)**	**Item 3 - Implantação e configuração da solução + Repasse de conhecimento hands-on (serviço)**	**Item 4 - Treinamento EAD de capacitação técnica para administração da solução (nº de alunos)**
TRT1	RJ	9.138	400	2	10
TRT2	SP	10.700	0	2	22
TRT3	MG	6.138	100	2	12
TRT4	RS	5.500	300	1	2
TRT5	BA	4.000	100	1	7
TRT6	PE	2.900	250	1	3
TRT7	CE	2.000	200	1	10
TRT8	PA/AP	2.850	150	1	5
TRT9	PR	4.763	100	1	3

TRT10	DF/TO	1.800	0	1	2
TRT11	AM/RR	1.700	400	1	6
TRT12	SC	3.000	220	1	22
TRT13	PB	1.700	300	1	6
TRT14	RO/AC	1.400	240	1	4
TRT15	SP	7.000	0	1	10
TRT16	MA	750	216	1	5
TRT17	ES	1.500	0	1	10
TRT18	GO	2.500	500	1	4
TRT19	AL	1.350	200	1	4
TRT20	SE	1.200	400	1	6
TRT21	RN	1.500	300	1	3
TRT22	PI	1.000	450	1	10
TRT23	MT	1.492	103	1	5
TRT24	MS	1.500	100	1	10
TST	DF	3.776	0	1	4
Total		81.157	5.029	28	185

8. LEVANTAMENTO DE MERCADO

BENS E SERVIÇOS DA SOLUÇÃO ESCOLHIDA					
Item	**Descrição**	**Unidade**	**Qtd.**	**Vlr. Unit.**	**Vlr. Total**
1	Licença de software de segurança para endpoints (estações de trabalho, dispositivos móveis e servidores físicos) + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	Nº de licenças	81.157	R$ 4,67/mês	R$ 18.192.153,12 (por 48 meses de contrato)
2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	Nº de licenças	5.029	R$ 8,15/mês	R$ 1.967.344,80 (por 48 meses de contrato)
3	Implantação e configuração da solução + Repasse de conhecimento hands-on	Serviço	28	R$ 26.000,00	R$ 728.000,00
4	Treinamento EAD de capacitação técnica para administração da solução.	Nº de alunos	185	R$ 3.880,00/aluno	R$ 717.800,00
Total Estimado					**R$ 21.605.297,92**

O **valor estimado para a aquisição pelo TRT13** é de **R$ 547.712,00** (quinhentos e quarenta e sete mil, setecentos e doze reais);

O **valor total estimado para a aquisição** é de **R$ 21.605.297,92** (vinte e um milhões, seiscentos e cinco mil, duzentos e noventa e sete reais e noventa e dois centavos).

9. NATUREZA DO OBJETO

Trata-se de objeto com características comuns e usuais encontradas no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, enquadrados nos termos da Lei n.º 10.520/2002 (instituiu o pregão), do Decreto n.º 3.555/2000 (regulamentou o pregão) e do Decreto n.º 10.024/2019 (regulamentou o pregão eletrônico).

10. PARCELAMENTO DO OBJETO

A solução é composta dos seguintes itens:

Lote	Item	Especificação
1	1	Licença de software de segurança para endpoints (estações de trabalho, dispositivos móveis e servidores físicos) + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.
	2	Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.
	3	Implantação e configuração da solução + Repasse de conhecimento hands-on
	4	Treinamento EAD de capacitação técnica para administração da solução.

A adjudicação se dará para um **único fornecedor**.

11. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR

Licitação:

- **Modalidade**: Pregão eletrônico, no Sistema de Registro de Preços;
- **Tipo**: Menor preço, com fundamento na legislação constante do subitem abaixo, bem como na Lei n.º 8.666/93, aplicada subsidiariamente;
- **Justificativa**: A modalidade foi escolhida por se tratar de serviço comum, em conformidade com Lei n.º 10.520/2002 (institui o pregão como modalidade de licitação), do Decreto n.º 3.555/2000 (regulamenta o pregão) e do Decreto n.º 10.024/2019(regulamenta o pregão na forma eletrônica). A adoção do Sistema de Registro de Preços (SRP) justifica-se com base no art. 3º, incisos III, do Decreto nº 7.892/2013, que preceitua que o SRP poderá ser adotado quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo;
- **Lei Complementar nº 123/06 e Lei 8.248/91**
    - Se estiverem participando do certame microempresas e empresas de pequeno porte, será observada a disciplina estabelecida nos artigos 44 e 45 da Lei Complementar 123/06, regulamentados pelo art. 5º do Decreto 8.538/15;
    - As Microempresas ou Empresa de Pequeno Porte participantes do procedimento licitatório deverão comprovar seu enquadramento e condições por meio de declaração específica, facultado ao Tribunal, se for o caso, promover diligência com a finalidade de comprovar o enquadramento do licitante como Microempresa ou Empresa de Pequeno Porte, nos termos do artigo 3.º, incisos I e II, da Lei Complementar n.º 123/2006, atualizada pela Lei Complementar n.º 147/2014, dos artigos 48, inciso I, e 49, inciso IV, da Lei

Complementar nº 123/2006, do art. 13, §2º, além do Decreto nº 8.538/2015, de 6 de outubro de 2015, que regulamenta o tratamento favorecido, diferenciado e simplificado para as microempresas e empresas de pequeno porte.

- **Critério Técnico de Habilitação**:
    1. O LICITANTE deverá comprovar ter fornecido licenças da solução com prestação de suporte, na quantidade de, pelo menos, **50% (cinquenta por cento) do quantitativo de licenças a ser registrado**;
        a. A comprovação dar-se-á pela apresentação de Declaração(ões), Certidão(ões) ou Atestado(s) emitido por pessoas jurídicas de Direito Público ou Privado, referente a fornecimento realizado em qualquer época ou local pela empresa licitante;
        b. Será admitida a apresentação de mais de um atestado que, somados, comprovem a experiência requerida da empresa no objeto em referência, contemplando todas as características qualitativas exigidas acima;
            i. **Justificativa**: Impedir a contratação de empresas incapazes de prestar suporte com a devida qualidade à Justiça do Trabalho, considerando que trata-se de contratação de porte nacional;
- **Critério de Julgamento**: Menor preço.
    - **Justificativa**: Por ser o critério determinado pelo art. 4º, inciso X, da Lei 10.520/2002, que disciplina as licitações na modalidade Pregão;
- **Ata de Registro de Preço:** A Ata de Registro de Preços terá **validade de 12 (doze) meses**, a partir da data de sua publicação no Diário Oficial da União. Não serão permitidas adesões à Ata de Registro de Preços. A referida Ata só poderá ser utilizada pelos órgãos ou entidades da Administração Pública Federal **que tenham participado do registro de preços**.

12. INFORMAÇÕES ACERCA DO IMPACTO AMBIENTAL

Não foram identificados impactos ambientais decorrentes da aquisição, por tratar-se de software.

13. CONFORMIDADE TÉCNICA E LEGAL

No escopo desta contratação, não foram identificados regulamentos ou normativos técnicos que precisem ser observados além do atendimento às especificações técnicas elencadas no **Anexo I - Especificações Técnicas** deste documento.

14. OBRIGAÇÕES CONTRATUAIS

14.1. Deveres e Responsabilidades da Contratante

- Proporcionar todas as condições para que a CONTRATADA possa desempenhar as atividades de acordo com as determinações do Contrato e deste Termo de Referência;
- Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais;

- 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;
- Zelar para que sejam mantidas, em compatibilidade com as obrigações assumidas pela CONTRATADA, todas as condições de habilitação e qualificação exigidas na contratação;
- Fornecer atestados de capacidade técnica, quando solicitado pela CONTRATADA, desde que atendidas às obrigações;
- 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;
- Para fins de formalização do ato de recebimento dos supramencionados documentos, de forma idêntica, a Contratada deverá informar a sua recepção;
- Prestar as informações e os esclarecimentos atinentes ao objeto que venham a ser solicitados pela Contratada;
- Efetuar o pagamento à contratada nos termos do subitem 15.6;
- Durante a realização do Certame, caberá ao Pregoeiro a realização de consulta ao Cadastro de Empresas Inidôneas e Suspensas – CEIS e ao Cadastro Nacional de Empresas Punidas – CNEP, emitindo os resultados respectivos, a fim de evitar a contratação de empresas que tenham sofrido penalidades que obstem a celebração da contratação pretendida, conforme previsão estabelecida pela Lei no 12.846/2013.
- Nomear Gestor e Fiscais Técnico e Administrativo para acompanhar e fiscalizar a execução do contrato;
- Receber os serviços prestados pela CONTRATADA desde que esteja em conformidade com o definido no contrato;
- Emitir pareceres no processo administrativo relativo à presente contratação, especialmente quanto à aplicação de penalidades e alterações contratuais, pelos gestores do contrato;

14.2. Deveres e Responsabilidades da Contratada

- Atender prontamente quaisquer orientações e exigências do Gestor do Contrato, inerentes à execução do objeto contratual;
- Coordenar, sob sua exclusiva responsabilidade, os profissionais necessários à prestação dos serviços objeto desta contratação;
- Designar formalmente preposto, apto a representá-la junto à contratante, em até **2 dias úteis** da assinatura do Contrato;
- Cumprir o Acordo de Nível de Serviço (SLA) estabelecido neste Termo de Referência, na seção 15.4 ("Níveis de Serviço");
- Submeter à aprovação do CONTRATANTE toda e qualquer alteração ocorrida nas especificações, em face de imposições técnicas, de cunho administrativo ou legal;
- 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;
- 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;

- 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;
- 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;
- Manter seus funcionários, quando nas dependências do CONTRATANTE, sujeitos às normas internas deste (segurança e disciplina), porém sem qualquer vínculo empregatício com o Órgão;
- Possibilitar a fiscalização do CONTRATANTE, no tocante à verificação das especificações exigidas neste Termo de Referência, prestando todos os esclarecimentos solicitados e atendendo às reclamações procedentes, caso ocorram;
- Comunicar ao CONTRATANTE, de imediato e por escrito, qualquer irregularidade verificada, para a adoção das medidas necessárias à sua regularização;
- Manter as condições de habilitação consignadas neste termo;
- Não transferir a terceiro, no todo ou em parte, o objeto da presente contratação;
- 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**;
- 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;
- 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;
- 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, podendo ser utilizado modelo em anexo;
- 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.

15. MODELO DE EXECUÇÃO E DE GESTÃO DO CONTRATO

15.1. Papéis e Responsabilidades

Papel	Entidade	Responsabilidade
Equipe de Apoio à Contratação	TRT13	Equipe responsável por subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes.
Equipe de Gestão da Contratação	TRT13	Equipe composta pelo Gestor do Contrato, responsável por gerir a execução contratual e, sempre que possível e necessário, pelos Fiscais Técnico e Administrativo, responsáveis por fiscalizar a execução contratual, consoante às atribuições regulamentares.
Fiscal Técnico do	TRT13	Servidor representante da Área de Tecnologia da Informação e Comunicação, indicado pela

Contrato		respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos técnicos da solução.
Fiscal Administrativo do Contrato	TRT13	Servidor representante da Área Administrativa, indicado pela respectiva autoridade competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.
Gestor do Contrato	TRT13	Servidor com atribuições gerenciais, técnicas ou operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente do órgão.
Preposto	Contratada	Funcionário representante da empresa contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao órgão contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual.

15.2. Dinâmica de Execução

15.2.1. 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	CRITÉRIO DE ACEITE
D0	-	Assinatura do contrato	TRT13 e CONTRATADA	Contrato assinado.
D1	D0 + 10	Reunião de Planejamento	TRT13 e CONTRATADA	Ata de reunião assinada.
D2	D0 + 20	Instalação e configuração da solução	CONTRATADA	Solução implantada e funcionando plenamente.
D3	D2 + 05	Recebimento Provisório	TRT13	Parecer do Fiscal Técnico.
D4	D3 + 05	Recebimento Definitivo	TRT13	Verificação do funcionamento e das especificações dos produtos e serviços entregues.

Caso a empresa verifique a impossibilidade de cumprir com o prazo de entrega estabelecido deverá encaminhar ao Tribunal solicitação de prorrogação, contendo:

a) Motivo para 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 ensejará o descumprimento de prazo, tais como: carta do fabricante/fornecedor, laudo técnico de terceiros, Boletim de Ocorrência de Sinistro, ou outro equivalente.

15.2.2. **Forma de Recebimento e Avaliação da Qualidade**

15.2.2.1. Os serviços devem ser prestados contínua e ininterruptamente, durante a vigência do contrato, obedecidos aos prazos e procedimentos especificados nos NÍVEIS DE SERVIÇO (item 15.4);

15.2.2.2. 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 13ª 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;

15.2.2.3. 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;

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

15.2.2.5. 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;

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

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

15.2.2.8. **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;

15.2.2.9. **Recebimento Definitivo (mensal - itens 1 e 2)**: Verificação dos serviços prestados e sua aderência às condições estabelecidas neste Termo de Referência.

15.2.2.10. **Recebimento Provisório (item 4)**: Conclusão do treinamento para os servidores do CONTRATANTE;

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

15.3. Instrumentos Formais de Solicitação dos bens e/ou serviços

O contrato assinado e a nota de empenho emitida são os instrumentos que autorizam o fornecimento.

15.4. Níveis de Serviço

- O atendimento aos chamados deverá estar disponível de segunda-feira a sexta-feira, no horário das 8h às 17h, horário de Brasília. A abertura de chamados pelo Contratante será efetuada por correio eletrônico, por sistema de controle de chamados ou por telefone. A abertura de chamado poderá ocorrer em qualquer horário por email ou sistema de controle de chamados, enquanto por telefone apenas no horário mencionado. No caso de abertura de chamado fora do horário estipulado, a contagem do prazo, para efeitos de nível de serviço (SLA), se dará no próximo dia útil;
- A assistência técnica em garantia deve garantir o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca);
- O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos produtos, módulos e programas referentes às plataformas de software e hardware (inclusive virtual) dos produtos;
- Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, instalação de novas versões, *patches* e *hotfixes*, análise de dúvidas sobre melhores práticas de configuração, entre outros;
- Os prazos de resposta para problemas ocorridos durante o período de suporte estão apresentados na tabela abaixo e são contados do recebimento da notificação de abertura do chamado:

Grau de impacto	Descrição	Tempo máximo para resposta inicial	Tempo máximo para solução
Nível 1 - Alto	Indisponibilidade de uso da solução	2 horas comerciais	1 dia útil
Nível 2 - Médio	Falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução	4 horas comerciais	2 dias úteis
Nível 3 - Baixo	Instalação, configuração, atualização de versões e implementações de novas funcionalidades	6 horas comerciais	3 dias úteis

- Automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções de produtos disponibilizadas pelo fabricante;
- A CONTRATADA deverá manter, durante toda a vigência do prazo de garantia, um "gerente técnico de contas". O "gerente técnico de contas" deverá ser o ponto de contato entre o FABRICANTE, CONTRATADA e CONTRATANTE para solucionar pendências e questões que não foram resolvidas pelo suporte técnico.

15.5. Forma de Comunicação e Acompanhamento da Execução do Contrato

As comunicações entre a CONTRATANTE e CONTRATADA se darão de forma periódica ou sob demanda, através de e-mail institucional e chamados telefônicos ou abertos via sistema próprio da CONTRATADA.

15.6. Forma de pagamento

- Para os itens 1 e 2, o pagamento será efetuado em **48 (quarenta e oito) parcelas mensais;**
- Para os itens 3 e 4, o pagamento será efetuado em **parcela única;**
- 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;
    - 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.
- 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;
- 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;
- Observar-se-á ainda se o CNPJ apresentado na Nota Fiscal é o mesmo constante dos documentos habilitatórios;
- Será efetuada por este Tribunal a retenção na fonte dos tributos e contribuições elencados na legislação em vigor, tais como, IR, CSLL, COFINS e PIS/PASEP;

- A retenção dos tributos não será efetuada caso o fornecedor apresente juntamente com a Nota Fiscal a comprovação de que é optante do Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES.

- Os preços dos serviços objeto deste contrato, 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;
- As Notas Fiscais, para fins de liquidação e pagamento das despesas, deverá ser entregue exclusivamente ao Gestor do Contrato, através do endereço eletrônico "setic-contratos@trt13.jus.br";
- 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;
- Será de inteira e única responsabilidade da contratada o recolhimento do ICMS referente aos bens junto ao órgão arrecadador do Estado, no que couber.
- 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;;
- Quando da ocorrência de eventuais atrasos de pagamento 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:

$$I = \frac{TX}{365} \text{ e } EM = I * N * VP$$

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.

15.7. Transferência de Conhecimento

15.7.1. Será realizada transferência de conhecimentos, mediante entrega de relatórios dos chamados atendidos, das alterações de versões implantadas, dos procedimentos indicados/adotados nos atendimentos e dos documentos produzidos durante a execução contratual. Todos os procedimentos realizados por meio de chamados abertos para o suporte devem ser acompanhados por, no mínimo, um profissional da equipe técnica do CONTRATANTE, cujo andamento deve ser posteriormente comunicado aos demais integrantes do quadro do Regional Trabalhista.

15.8. Propriedade, Sigilo e Restrições

15.8.1. Os conhecimentos, dados e informações de propriedade do CONTRATANTE, tanto tecnológicos como administrativos, tais como: produtos, sistemas, técnicas, estratégias, métodos de operação e todos e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade;

15.8.2. Estas informações poderão ser utilizadas, só e exclusivamente, no cumprimento da execução das cláusulas e condições estabelecidas no contrato, sendo expressamente vedado à CONTRATADA:

a) Utilizá-las para fins não previstos no instrumento contratual;
b) Repassá-las a terceiros e/ou empregados não vinculados diretamente à execução do objeto contratado.

15.9. Qualificação técnica/operacional

15.9.1. Pelo menos 1 (um) profissional com certificação ou documento/atestado técnico emitido **pelo fabricante da solução** contratada. Esta solicitação visa garantir que a CONTRATADA tenha plenas condições de elaborar/acompanhar o processo de instalação/configuração do objeto da licitação, assim como manter o nível de suporte técnico necessário durante toda a vigência do contrato;

15.9.2. A empresa deverá apresentar um documento que comprove ser REVENDA AUTORIZADA do fabricante do software

15.9.2.1. Tal exigência visa proteger o alto investimento feito pela Administração na aquisição da solução. Considerando que o escopo do projeto inclui não somente o fornecimento de licenças, mas também o suporte técnico durante 48 meses e que se trata de software fundamental para manutenção da segurança dos dados da instituição, exige-se a declaração de revenda autorizada, visto que tais fornecedores são obrigados a cumprir uma série de requisitos de qualidade determinados pelos fabricantes.

15.10. Situações que Caracterizam Descumprimento das Obrigações Contratuais

15.10.1. 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:

a) apresentar documentação falsa;
b) fraudar a execução do contrato;
c) comportar-se de modo inidôneo;
d) cometer fraude fiscal; ou
e) fizer declaração falsa.

15.10.2. 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;

15.10.3. 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;

15.10.4. 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

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 deste Termo de Referência e demais disposições contratuais.	3	4
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 à Execução do Objeto		
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 deste Termo de Referência para o nível 1 de impacto.	3	4
Deixar de cumprir os prazos estabelecidos no subitem 15.4 deste Termo de Referência para o nível 2 de impacto.	2	3
Deixar de cumprir os prazos estabelecidos no subitem 15.4 deste Termo de Referência para o nível 3 de impacto.	1	2
Deixar de cumprir o cronograma de treinamento, a ser definido junto à CONTRATANTE	1	2

16. GARANTIA DE EXECUÇÃO DO CONTRATO

16.1. No prazo de **10 (dez) 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:

a) Caução em dinheiro ou em títulos da dívida pública;

b) Fiança bancária;

c) Seguro garantia.

16.2. 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;

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

16.4. 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;

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

16.6. 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.

17. REQUISITOS TÉCNICOS ESPECÍFICOS

As especificações técnicas dos itens previstos neste documento a serem adquiridos estão descritas no **ANEXO I - ESPECIFICAÇÕES TÉCNICAS**.

18. DA DOTAÇÃO ORÇAMENTÁRIA

Item	Natureza de Despesa	Fonte de Recurso
Item 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**.	33.90.40.11 - SUPORTE DE INFRAESTRUTURA DE TIC	Descentralizado
Item 2 - Licença de software de segurança para ambiente virtualizado + Console de Gerenciamento / Garantia / Atualizações / Suporte Técnico / Manutenção Preventiva e Corretiva por **48 meses**.	33.90.40.11 - SUPORTE DE INFRAESTRUTURA DE TIC	Descentralizado
Item 3 - Implantação e configuração da solução + Repasse de conhecimento hands-on	33.90.40.21 - SERVICOS TECNICOS DE PROFISSIONAIS DE TIC - PJ	Descentralizado
Item 4 - Treinamento EAD de capacitação técnica para administração da solução.	33.90.40.20 - TREINAMENTO/CAPACITACAO EM TIC	Descentralizado

19. DA VIGÊNCIA DO CONTRATO

A vigência do Contrato será 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.

20. MODELOS (TEMPLATES)

No link abaixo podem ser verificados os modelos atualizados para a fase de execução da contratação (gestão do contrato), contemplando:

- Plano de Fiscalização;
- Termo de Ciência;
- Termo de Compromisso;
- Termo de Recebimento Provisório;
- Termo de Recebimento Definitivo.

https://www.trt13.jus.br/institucional/governanca/projetos-e-servicos/processos-de-tic/processo-de-contratacao/modelos-de-documentos

21. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

A Equipe de Planejamento da Contratação, composta pelos **Integrantes Demandante**, **Técnico** e **Administrativo**, designados por meio da PORTARIA TRT GDG Nº **67/2020**, abaixo elencados, **assina e data este documento eletronicamente**:

Papel	Nome	Setor	Ramal	E-mail
Integrante Demandante	Raimundo José Campos Junior	SETIC	6055	rjcampos@trt13.jus.br
Integrante Técnico	Alessandra Mendes da Silva	SETIC	6022	asilva@trt13.jus.br
Integrante Técnico	Rodrigo Mafra	SETIC	6150	rmafra@trt13.jus.br
Integrante Administrativo	Hérika Felix Brito	SADM	6011	hbrito@trt13.jus.br

Além da equipe de planejamento, a **Autoridade da Área Demandante**, abaixo informada, aprova este documento, **assinando-o e datando-o eletronicamente**:

Papel	Nome	Setor	Ramal	E-mail
Autoridade da Área Demandante	Rodrigo Cartaxo Marques Duarte	SETIC	6057	rcduarte@trt13.jus.br

ANEXO I - ESPECIFICAÇÕES TÉCNICAS

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

1. Requisitos Gerais – Comuns aos itens 1 e 2

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

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

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.

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

1.3.

1.4. O Console de Gerenciamento deve conter:

1.4.1. Painel para monitoramento;

1.4.2. Capacidade de criação de relatórios;

1.4.3. Mecanismo para envio de notificações administrativas (e-mail);

1.5. Deve permitir inventário das máquinas gerenciadas pela solução;

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

1.7.

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

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

1.8.2. Capacidade de exportar relatórios para, no mínimo 2, dos seguintes tipos de arquivos: PDF, HTML e CSV;

1.8.3. Capacidade de enviar e-mails para contas específicas, em caso de algum evento;

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

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

1.8.4.2. Data e horário da última verificação executada na máquina;

1.8.4.3. Se a solução está instalado;

1.8.4.4. Versão do antivírus instalado na máquina gerenciada;

1.8.4.5. Se o antivírus está atualizado;

1.8.4.6. Nome do computador;

1.8.4.7. Domínio ou grupo de trabalho do computador;

1.8.4.8. Sistema operacional e Service Pack/Build;

1.8.4.9.

1.8.4.10. Endereço IP.

1.9. 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;

1.10. 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);

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

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

1.13. 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;

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

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

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

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

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

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

1.20. Deve armazenar histórico das alterações feitas em políticas;

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

1.21.1. Nome do computador;

1.21.2.

1.21.3. Range de IP;

1.21.4. Sistema Operacional;

1.21.5.

1.22. 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;

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

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

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

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

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

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

1.28.1. Detalhes do ataque;

1.28.2. IOCs;

1.28.3. Detalhes do Impacto no ambiente;

1.28.4.
1.28.5. Endpoints afetados;
1.28.6. Comportamento da ameaça.

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

2.1. Requisitos Gerais

2.1.1. Prover segurança para as estações de trabalho (endpoints), sejam físicas ou em ambiente virtualizado;
2.1.2. Se comunicar com console central de gerenciamento, de forma que seja possível gerenciar todas as funcionalidades;
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;
2.1.4. Identificar e proteger contra eventuais vulnerabilidades dos sistemas operacionais e aplicações;
2.1.5. Deve detectar e eliminar programas maliciosos em:
2.1.5.1. Processos Em Execução Em Memória principal (RAM);
2.1.5.2. Arquivos Executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
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;
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.
2.1.6. Capacidade de detecção heurística de malwares desconhecidos;
2.1.7. Possuir tecnologia de Machine Learning de pre-execution, run time machine e post-execution;
2.1.8. Deve prover, no mínimo, as seguintes proteções:
2.1.8.1. Antivírus de arquivos;
2.1.8.2. Antivírus web (verificação de sites e downloads contra malwares);
2.1.8.3. Firewall de host com HIPS (Host Intrusion Prevention System) e/ou HIDS (Host Intrusion Detection System);
2.1.8.4. Proteção contra ataques aos serviços/processos do antivírus;
2.1.8.5. Controle de dispositivos;
2.1.8.6. Controle de execução de aplicativos;
2.1.8.7. Controle de acesso a sites por categorias (Adulto, Jogos, etc);
2.1.8.8. Prevenção contra exploração de vulnerabilidades.
2.1.8.9. Capacidade de integração com a Antimalware Scan Interface (AMSI).
2.1.9. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota.

2.2. Detalhamento das proteções:

2.2.1. Antivírus de arquivos:

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;

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;

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

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

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

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

2.2.1.7. Possibilidade de definir frequência de varredura;

2.2.1.8.

2.2.1.9. 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;

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

2.2.2. Antivírus web:

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

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

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

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

2.2.3. Firewall de host com HIPS e/ou HIDS

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

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;

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

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.

2.2.4. Proteção contra Ameaças Avançadas

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

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;

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

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

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

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

2.2.4.6.1. Acesso local a partir de cookies;

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

2.2.4.6.3. Criação de threads em outro processo;

2.2.4.6.4. Desativação de executáveis críticos do sistema operacional;

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

2.2.4.6.6. Gravação e Leitura na memória de outro processo;

2.2.4.6.7. Modificação da política de firewall do Windows;

2.2.4.6.8. Modificação da pasta de tarefas do Windows;

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

2.2.4.6.10. Modificação de arquivos executáveis portáteis;

2.2.4.6.11. Modificação de bit de atributo oculto;

2.2.4.6.12. Modificação de bit de atributo somente leitura;

2.2.4.6.13. Modificação de entradas de registro de DLL AppInit;

2.2.4.6.14. Modificação de locais do registro de inicialização;

2.2.4.6.15. Modificação de pastas de dados de usuários;

2.2.4.6.16. Modificação do local do Registro de Serviços;

2.2.4.6.17. Suspensão de um processo;

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

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

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;

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

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;

2.2.4.12. Utilizar técnicas de machine learning para detecção de ameaças

2.2.5. Controle de dispositivos:

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

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;

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

2.2.6. Controle de execução de aplicativos:

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;
2.2.6.2. Deve ser capaz de realizar um inventário das estações de trabalho protegidas informando todos os executáveis presentes;
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;
2.2.6.4. Ao detectar um executável, a solução deverá consultar a Solução de reputação de arquivos e compartilhamento de informações de segurança;
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;
2.2.6.6. Deve ser possível criar uma imagem base para a criação de uma política geral;
2.2.6.7. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando-se à novas aplicações instaladas na máquina;
2.2.6.8. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA- 1).
2.2.6.9. A solução deve suportar as seguintes modalidades de proteção:
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;
2.2.6.9.2. Criação de uma lista de aplicações não autorizadas que não podem ser executadas;
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.
2.2.6.10. Deve ser capaz de proteger em modo standalone - online ou offline;
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;
2.2.6.12.
2.2.6.13.
2.2.6.14. Permitir o bloqueio de aplicações e os processos que a aplicação interage;
2.2.6.15. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;
2.2.6.16. Permitir monitoração de Hooking de aplicações;
2.2.7. Proteção contra ransomwares:
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;
2.2.7.2. Monitoramento de pastas compartilhadas no ambiente Windows, rastreando o estado dos arquivos armazenados e os protegendo;
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.

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

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

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

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;

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

2.3.5.

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

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

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

2.3.8.1. Reputação local;

2.3.8.2. Reputação do centro de inteligência.

2.3.9.

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

2.3.10.1. Rastrear em quais estações o arquivo foi executado;

2.3.10.2. Identificar o arquivo como confiável;

2.3.10.3. Identificar o arquivo como desconhecido;

2.3.10.4. Identificar o arquivo como malicioso;

2.3.10.5. Analisar o certificado associado ao arquivo;

2.3.10.6. Identificar o certificado associado como confiável ou malicioso.

2.3.11.

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

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

2.3.14.

2.4. Módulo de proteção para dispositivos móveis

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;

2.4.2. Características Gerais:

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;

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

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;

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

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

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;
2.4.2.7. Deverá ser compatível com os sistemas operacionais iOS e Android;
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.
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;
2.4.2.10. Deverá possuir as seguintes características mínimas de proteção:
2.4.2.10.1. Proteção contra Malwares:
2.4.2.10.1.1. Proteção em tempo real contra malwares conhecidos e desconhecidos;
2.4.2.10.2. Defesa física
2.4.2.10.2.1. Identificação de upgrades do sistema operacional;
2.4.2.10.2.2. Identificação de dispositivo com root.
2.4.2.11. Deverá possuir integração com solução de SIEM de mercado;
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;

2.5. Compatibilidade

2.5.1. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações de trabalho:
2.5.1.1. Microsoft Windows 8 (e suas edições);
2.5.1.2. Microsoft Windows 8.1 (e suas edições);
2.5.1.3. Microsoft Windows 10 (e suas edições);
2.5.1.4. Ser compatível para instalação em sistemas legados em Windows 7.
2.5.2. O software de segurança deve ser compatível com as seguintes versões de sistemas operacionais Windows para servidores:
2.5.2.1. Microsoft Windows Server 2012 (e suas edições);
2.5.2.2. Microsoft Windows Server 2012 R2 (e suas edições);
2.5.2.3. Microsoft Windows Server 2016 (e suas edições);
2.5.2.4. Microsoft Windows Server 2019 (e suas edições).
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:
2.5.3.1. Red Hat Enterprise 7.x e superior, 32 e 64bits;
2.5.3.2. SUSE Linux Enterprise Server 12.x e superior, 32 e 64bits;
2.5.3.3. Ubuntu 16.04 e superior, 32 e 64bits;
2.5.3.4. CentOS 7.x e superior, 32 e 64bits;
2.5.3.5. Oracle Linux 7.x e superior, 32 e 64bits;

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

3.1. Requisitos Gerais

3.1.1. Ser totalmente compatível e homologada para gerenciamento de máquinas virtuais nos ambientes VMware ESXi e Hyper-V;
3.1.2. Deve prover, no mínimo, as seguintes proteções:
3.1.2.1. Antivírus de arquivos que verifique todos os arquivos criados, acessados ou modificados;

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

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

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

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

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

3.1.4.3. Leitura de configurações;

3.1.4.4. Modificação de configurações.

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

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

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;

3.1.8. Capacidade de verificar objetos usando heurística;

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

3.2. Compatibilidade

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

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

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

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

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

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

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

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

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

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

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

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

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;

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;

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;

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;

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

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;

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

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

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;

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.

5. Item 4 - Treinamento e Atualização Tecnológica

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;

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

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

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;

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

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

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;

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

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

5.9.1. Instalação do ambiente;

5.9.2. Manutenção básica, intermediária e avançada;

5.9.3. Configurações básicas e avançadas;

5.9.4. Verificação de alertas e erros;

5.9.5. Monitoramento e relatórios.

6. CONDIÇÕES DE FORNECIMENTO

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.

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).

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

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

6.2. O TRT13, 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.

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