TRIBUNAL SUPERIOR DO TRABALHO
AVISO DE ALTERAÇÕES
Edital do Pregão Eletrônico n.º 031/2020

(Regido pela Lei Complementar 123/06, pela Lei 10.520/02, pelos Decretos 10.024/19 e 8.538/15 e subsidiariamente pelas Leis 8.078/90, 8.666/93, 9.784/99 e alterações).

Objeto: **Aquisição e instalação de solução de segurança Firewall.**

Data de abertura da sessão pública:
03/09/2020 às 14h30 no sítio www.comprasgovernamentais.gov.br

Tipo: Menor preço	**Modo de disputa:** Aberto	**Exclusiva ME/EPP?** ☐Sim ☒Não	**Reserva de cota exclusiva ME/EPP?** ☐Sim ☒Não
Processo: 501.233/2020-5			
Valor total estimado: R$ 2.420.945,38		**Apresentação de amostra?** ☐Sim ☒Não	**Margem ou direito de preferência?** ☐ Sim ☒ Não
Regime de execução: Empreitada por preço global.			

Pedidos de esclarecimento e impugnações:
Até às 19h de 31/08/2020.

Os pedidos de esclarecimento e as impugnações referentes a este procedimento devem ser encaminhados exclusivamente por meio eletrônico via internet, para o endereço cpl@tst.jus.br.

Documentos de habilitação: (veja seção 8)

Requisitos básicos:	**Requisitos específicos:**
1. SICAF* ou documentos equivalentes; 2. Comprovação de capital social não inferior a 10%, quando o índice de liquidez corrente for igual ou inferior a 1. *Será emitido pelo pregoeiro durante a sessão pública.	Apresentação de, pelo menos, um atestado de capacidade técnica compatível com o objeto desta licitação.

Endereço da Coordenadoria de Licitações e Contratos: SAFS quadra 8, conjunto A, bloco A, sala A3.41. Brasília – DF. CEP: 70070-943.
Retire o edital e acompanhe esta licitação e seus atos na internet pelos portais www.tst.jus.br e www.comprasgovernamentais.gov.br

1. Objeto do Aviso

1.1. A pregoeira informa que, conforme nova redação dada pelo Edital n.º 031/2020 que acompanha este aviso, foram alterados os itens 13.2.1, 13.2.2, 14.1.1.2 e excluído o item 14.1.1.3 do edital; foram também alteradas as especificações constantes dos itens R.HS3, R.HS28, R.HS54, R.HS58, R.HS171 e R.SG7 do Anexo I do Termo de Referência; e excluídos os itens R.HS72, R.HS269, R.HS270, tendo sido renumerados os itens na sequência.

1.2. Ficam mantidas as demais condições.

1.3. Quaisquer outros elementos necessários ao perfeito entendimento deste edital poderão ser obtidos junto à Coordenadoria de Licitações e Contratos, exclusivamente por meio do endereço eletrônico cpl@tst.jus.br.

1.4. Esta licitação poderá ser acompanhada nos portais www.tst.jus.br e www.comprasgovernamentais.gov.br, locais onde são divulgados os prazos e demais informações do certame.

JUMARA CRISTINA SILVA CERQUEIRA

Assinado de forma digital por JUMARA CRISTINA SILVA CERQUEIRA
DN: c=BR, o=ICP-Brasil, ou=Pessoa Fisica A3, ou=ARSERPRO, ou=Autoridade Certificadora SERPROACF, cn=JUMARA CRISTINA SILVA CERQUEIRA
Dados: 2020.08.21 11:12:00 -03'00'

Jumara Cristina Silva Cerqueira

Pregoeira

TRIBUNAL SUPERIOR DO TRABALHO
Edital do Pregão Eletrônico n.º 031/2020

(Regido pela Lei Complementar 123/06, pela Lei 10.520/02, pelos Decretos 10.024/19 e 8.538/15 e subsidiariamente pelas Leis 8.078/90, 8.666/93, 9.784/99 e alterações).

Objeto: **Aquisição e instalação de solução de segurança Firewall.**

Data de abertura da sessão pública:
03/09/2020 às 14h30 no sítio www.comprasgovernamentais.gov.br

Tipo: Menor preço	**Modo de disputa:** Aberto	**Exclusiva ME/EPP?** ☐Sim ☒Não	**Reserva de cota exclusiva ME/EPP?** ☐Sim ☒Não
Processo: 501.233/2020-5			
Valor total estimado: R$ 2.420.945,38		**Apresentação de amostra?** ☐Sim ☒Não	**Margem ou direito de preferência?** ☐ Sim ☒ Não
Regime de execução: Empreitada por preço global.			

Pedidos de esclarecimento e impugnações:
Até às 19h de 31/08/2020.

Os pedidos de esclarecimento e as impugnações referentes a este procedimento devem ser encaminhados exclusivamente por meio eletrônico via internet, para o endereço cpl@tst.jus.br.

Documentos de habilitação: (veja seção 8)

Requisitos básicos:	**Requisitos específicos:**
3. SICAF* ou documentos equivalentes; 4. Comprovação de capital social não inferior a 10%, quando o índice de liquidez corrente for igual ou inferior a 1. *Será emitido pelo pregoeiro durante a sessão pública.	Apresentação de, pelo menos, um atestado de capacidade técnica compatível com o objeto desta licitação.

Endereço da Coordenadoria de Licitações e Contratos: SAFS quadra 8, conjunto A, bloco A, sala A3.41. Brasília – DF. CEP: 70070-943.
Retire o edital e acompanhe esta licitação e seus atos na internet pelos portais www.tst.jus.br e www.comprasgovernamentais.gov.br

1. Objeto da Licitação

1.1. O objeto deste certame é a aquisição e instalação de solução de segurança para redes de dados do tipo Next Generation Firewall de alta disponibilidade, compreendendo: sistema de detecção e prevenção de intrusão do TIPO IPS/IDS, gerenciamento centralizado e integrado, controle de ameaças, filtro de URL, controle de aplicação, suporte e garantia do fabricante, assinaturas de proteção e suporte técnico em repositório mundial do fabricante, suporte técnico do fabricante local e/ou remoto, incluindo serviços de instalação e treinamento.

Grupo 1 – Itens 1 a 4				
Item	**Especificação**	**Unidade**	**Quantidade**	**Valor total estimado R$**
1	Cluster Firewall NGFW **CATMAT: 320365**	Equipamento	1	1.851.945,38
2	Sistema de Gerenciamento – Next Generation Security Management **CATMAT: 320365**	Unidade	1	358.500,00
3	Serviço de Instalação e Configuração **CATSER: 26972**	Serviço	1	129.000,00
4	Treinamento especializado para 5 (cinco) alunos **CATSER: 3840**	Turma	1	81.500,00

1.2. É parte integrante deste edital o Termo de Referência, cujo anexo é:

1.2.1. Anexo I – Especificação técnica do objeto;

1.3. Os equipamentos deverão ser acondicionados em suas embalagens originais, lacradas e apropriadas para armazenamento, com a sua identificação, fazendo constar sua descrição e incluindo, quando cabíveis: marca, fabricante, data de fabricação, validade e outras especificações de acordo com suas características.

2. Condições para Participação

2.1. Poderão participar deste pregão os interessados que atenderem a todas as exigências constantes deste edital, que estiverem previamente credenciados perante a Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão, provedor do sistema eletrônico, cuja comunicação se dá pela Internet.

2.1.1. Para ter acesso ao sistema eletrônico, os interessados em participar do pregão deverão dispor de chave de identificação e senha que poderão ser utilizadas em qualquer pregão eletrônico, salvo quando cancelada por solicitação do credenciado ou em virtude de seu descadastramento perante o SICAF.

2.1.2. O uso da senha de acesso pelo licitante é de sua inteira responsabilidade bem assim quaisquer transações efetuadas diretamente ou por seu representante, e não caberá ao provedor do sistema ou ao TST a responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

2.1.3. A perda da senha ou a quebra do sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.

2.1.4. O credenciamento perante o provedor do sistema implica a responsabilidade legal do licitante e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

2.2. Ficam impedidos de participar desta licitação:

2.2.1. Os interessados que se encontrem sob falência, concurso de credores, dissolução, liquidação ou em regime de consórcio, qualquer que seja sua forma de constituição e as empresas estrangeiras que não funcionem no país;

2.2.2. Aqueles que tenham sido declarados inidôneos para licitar ou contratar com a Administração Pública ou punidos com suspensão do direito de licitar e contratar pelo TST, com base na Lei n.º 8.666/1993; ou impedidos de licitar e contratar com a União, com base na Lei n.º 10.520/2002 (TCU Acórdãos 842/2013, 3439/2012, 3243/2012 e 2242/2013, todos do Plenário).

2.2.3. A pessoa jurídica cujo(s) sócio(s) que compõe(m) seu quadro societário incorra(m) na vedação constante do inciso VI do art. 2º da Resolução CNJ 7/2005, acrescentado pela Resolução CNJ 229/2016.

2.3. O pregoeiro realizará a Consulta Consolidada de Pessoa Jurídica do Tribunal de Contas da União, que abrange o cadastro do CNJ, do CEIS, do próprio TCU e o CNEP, a fim de evitar a contratação de empresas que tenham sofrido penalidades que obstem a celebração do contrato pretendido.

3. Credenciamento dos Representantes

3.1. O credenciamento do licitante, bem assim a sua manutenção, dependerá de registro atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 10 do Decreto nº 10.024/2019.

3.1.1. Caberá ao licitante interessado em participar do pregão eletrônico credenciar-se no SICAF, conforme disposto no inciso I do art. 19 do Decreto 10.024/2019.

3.2. O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico e assumirá como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, excluída a

responsabilidade do provedor do sistema ou deste Tribunal por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

4. Apresentação da Proposta e dos Documentos de Habilitação

4.1. As propostas deverão ser formuladas e encaminhadas exclusivamente por meio do sistema eletrônico, concomitantemente com os documentos de habilitação exigidos neste edital, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

4.1.1. As propostas deverão consignar no(s) campo(s) apropriado(s) do sistema o preço total, expresso em reais, incluindo todos os impostos, taxas, fretes, e demais encargos indispensáveis ao perfeito cumprimento das obrigações contratuais.

4.1.2. Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema.

4.1.3. Os documentos de habilitação abrangidos pelo SICAF serão verificados pelo pregoeiro durante a sessão pública, nos termos do *caput* do art. 43 do Decreto 10.024/19.

4.2. Os interessados deverão cotar **todos os itens do grupo**, sob pena de desclassificação.

4.3. A proposta deverá ainda especificar, quando cabíveis, nos campos apropriados do sistema: marca, modelo, fabricante, data de fabricação, validade, garantia e demais referências que identifiquem o produto cotado, ficando o proponente, em caso de omissão, obrigado a fornecer o bem indicado pelo TST.

4.4. No campo “Descrição Detalhada do Objeto Ofertado” devem ser incluídas todas as informações necessárias ao perfeito detalhamento do objeto e, ainda, as seguintes informações relativas à proposta, cuja omissão e/ou contrariedade implica a aceitação dos prazos indicados:

4.4.1. Prazo de entrega e instalação dos equipamentos de, no máximo, sessenta dias corridos contados da assinatura do contrato;

4.4.2. Prazo de garantia dos equipamentos de, no mínimo, sessenta meses contados do recebimento definitivo do objeto;

4.4.3. Prazo de validade da proposta de, no mínimo, noventa dias.

4.5. Serão desclassificadas as propostas que comprovadamente cotarem objeto diverso daquele requerido nesta licitação, **que deixarem de cotar todos os itens de cada grupo** ou as que desatendam às exigências deste edital.

4.6. Os licitantes, no ato de envio de suas propostas, devem encaminhar, de forma virtual, utilizando a funcionalidade existente no sistema de pregão eletrônico, as seguintes declarações:

4.6.1. Inexistência de fato superveniente que o impeça de participar do certame;

4.6.2. Cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal;

4.6.3. Concordância com as condições estabelecidas neste edital e que atende aos requisitos de habilitação;

4.6.4. Atendimento aos requisitos do art. 3º da Lei Complementar n.º 123/2006, no caso de microempresas e empresas de pequeno porte.

4.7. A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará o licitante às sanções previstas neste edital.

4.8. O licitante melhor classificado, após a fase de lances, deverá encaminhar, ainda, atendendo convocação do pregoeiro, declaração, conforme modelo do Anexo II (disponível no seguinte link: http://bit.ly/decNEPlicit), a fim de resguardar este órgão quanto à prática de nepotismo vedada pela Resolução CNJ nº 7, de 18/10/2005, com as alterações introduzidas pela Resolução 229, de 22/06/2016.

4.8.1. A Declaração deverá ser reapresentada no momento da assinatura do contrato, firmada por todos os sócios que compõem o quadro societário do licitante, conforme modelo constante do Anexo III (http://bit.ly/decNEPcont).

5. Critério de Aceitabilidade dos Preços

5.1. Os preços deverão ser cotados em reais, com duas casas decimais, sob pena de serem truncados.

5.2. Não serão aceitas propostas cujos valores **de cada um dos itens ou do grupo sejam superiores aos valores estimados** ou com preços manifestamente inexequíveis.

5.2.1. Somente poderá ser considerado excessivo qualquer preço após o encerramento da etapa de lances e, quando formulada contraproposta pelo Pregoeiro, após sua recusa ou no caso de omissão por parte do respectivo proponente.

5.3. Considera-se inexequível a proposta que, comprovadamente, for insuficiente para a cobertura dos custos da contratação, apresente preços simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da licitação não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

5.3.1. Quando o licitante apresentar preço final inferior a 30% (trinta por cento) da média dos preços ofertados para o item será obrigatória a realização de diligências para o exame da proposta.

5.3.2. O ônus da prova da exequibilidade dos preços cotados incumbe ao autor da proposta, no prazo de três dias úteis contados da notificação.

6. Sessão Pública do Pregão Eletrônico

6.1. A sessão pública deste pregão eletrônico, conduzida pelo pregoeiro designado, ocorrerá em data e hora indicadas exclusivamente no sistema eletrônico e obedecerá ao rito estabelecido nos Decretos 10.024/2019 e 8.538/15.

6.1.1. Por força do disposto no art. 19, inciso IV do Decreto 10.024/2019, os licitantes estão obrigados a acompanhar as operações no sistema eletrônico durante a licitação, responsabilizando-se pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão.

6.2. Aberta a sessão pública, o pregoeiro verificará as propostas apresentadas e desclassificará aquelas que estejam em desconformidade com os requisitos estabelecidos neste edital.

6.2.1. O pregoeiro abrirá todos os itens e procederá a análise das propostas de cada um deles.

6.2.2. A desclassificação de um único item implicará a desclassificação da proposta global.

6.2.3. A desclassificação de proposta será sempre fundamentada e registrada no sistema, com acompanhamento, em tempo real, por todos os participantes.

6.2.4. O desatendimento de exigências formais não essenciais não importará no afastamento da Licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão de sua proposta, durante a realização da Sessão Pública.

6.3. O sistema ordenará automaticamente somente as propostas classificadas pelo pregoeiro, as quais participarão da fase de lances.

6.4. O pregoeiro dará início à fase competitiva, quando então os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico.

6.5. Os licitantes poderão oferecer lances sucessivos e inferiores aos últimos por eles ofertados e registrados pelo sistema, observado o intervalo mínimo de diferença de valores entre os lances de R$ 800,00 (oitocentos reais), que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta, conforme disposto no parágrafo único do art. 31 do Decreto 10.024/2019.

6.5.1. Caso haja dois ou mais lances iguais, prevalecerá aquele que for recebido e registrado primeiro.

6.6. Na fase de lances, a disputa será por item e a classificação final será pelo valor global do grupo.

6.6.1. Não se recomenda concentrar o esforço de redução em apenas um dos itens que integram o grupo, pois a incompatibilidade de um deles com o respectivo valor estimado pode levar à desclassificação da respectiva empresa proponente, nos termos do item 7.7.1.

6.7. **MODO DE DISPUTA – ABERTO:** Será adotado para o envio de lances o modo de disputa aberto, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.7.1. A etapa de envio de lances durará dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos.

6.7.2. A prorrogação automática da etapa de envio de lances será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período, inclusive quando se tratar de lances intermediários.

6.7.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a etapa de envio de lances será encerrada automaticamente.

6.7.4. Encerrada a etapa de envio de lances sem prorrogação automática pelo sistema, o pregoeiro, mediante justificativa, poderá admitir o reinício dessa etapa, em prol da consecução do melhor preço disposto no parágrafo único do art. 7º do Decreto 10.024/2019.

6.8. A cada lance ofertado por item, o Sistema atualizará automaticamente o valor global do grupo.

6.8.1. A empresa que ofertar o menor valor global para o grupo será classificada em primeiro lugar pelo critério de Julgamento por Preço Global – Lote.

6.9. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado que tenha sido apresentado pelos demais licitantes, vedada a identificação do detentor do lance.

6.10. No caso de desconexão do pregoeiro durante a etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

6.11. **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.**

7. Julgamento das Propostas e Habilitação

7.1. Encerrada a etapa de lances, o pregoeiro irá verificar se os documentos de habilitação foram enviados concomitantemente com a proposta, conforme previsto no item 4.1. Em seguida, fará contraproposta ao licitante que tenha apresentado lance mais vantajoso pelo sistema eletrônico, para que seja obtida melhor proposta, observado o critério de julgamento, sendo inadmissível negociar condições diferentes daquelas previstas no edital.

7.1.1. A negociação será realizada exclusivamente pelo canal de comunicação (chat) existente no sistema e poderá ser acompanhada pelos demais licitantes.

7.1.2. O pregoeiro, utilizando a funcionalidade de “convocação de anexos” existente no sistema de pregão eletrônico, notificará o licitante melhor classificado a enviar a proposta e a Declaração de que trata o item 4.8, no prazo de 24 (vinte e quatro) horas.

7.2. As propostas que resultarem preços manifestamente inexequíveis serão desclassificadas.

7.2.1. Consideram-se preços manifestamente inexequíveis aqueles que, comprovadamente, forem insuficientes para a cobertura dos custos decorrentes da contratação pretendida.

7.2.2. Se houver indícios de inexequibilidade da proposta de preço, ou em caso de necessidade de esclarecimentos complementares, poderão ser efetuadas outras diligências.

7.3. **PROPOSTA TÉCNICA - Juntamente com a proposta de preços, deverá ser apresentada proposta técnica, com o objetivo de assegurar que os produtos ofertados cumprem os requisitos exigidos neste edital e em seus anexos.**

7.3.1. A proposta técnica deve conter a descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas;

7.3.2. Apresentar na proposta a indicação detalhada do equipamento ofertado citando a marca, modelo, tipo e fabricante;

7.3.3. A proposta técnica deverá conter, obrigatoriamente, tabela de comprovação técnica apresentada conforme modelo abaixo. É necessária a especificação de todos os itens contidos noo Anexo I do Termo de Referência e a apresentação da documentação comprobatória com indicação da página e com informações das funcionalidades e características exigidas, grifadas. Salienta-se que todos os itens da tabela devem ser devidamente preenchidos.

Nº Requisito no TR	Descrição da característica ou funcionalidade exigida	Documento do fabricante (nome)	Página(s)	Atende ao Requisito (sim/não)
R.HS1	.....	.....	.....	.....

7.3.4. Serão considerados documentos oficiais para comprovação técnica: catálogos, folders, prospectos e manuais;

7.3.5. Para os documentos do fabricante, é mandatória a comprovação que se trata de documento oficial fornecido pelo fabricante ao mercado, sendo comprovação suficiente desse requisito o link para o acesso ao documento no site do fabricante;

7.3.6. Havendo divergência entra as características técnicas descritas na proposta da licitante e as disponibilizadas pelo fabricante, prevalecerão os informes do fabricante, salvo os casos específicos em que o licitante esclareça os motivos da divergência e que sejam aceitos pelo TST;

7.3.7. Os documentos técnicos fornecidos que não apresentarem numeração de página deverão ser numerados manualmente de forma visível pela Licitante, no canto inferior direito;

7.3.8. Além da indicação da página da documentação fornecida na qual se encontra a comprovação de cada funcionalidade ou característica técnica exigida para cada item, a correspondente comprovação deverá ser necessariamente grifada ou destacada com marca texto;

7.4. O licitante que não apresentar a documentação, apresentar fora do prazo estabelecido ou apresentá-la em desacordo com as especificações será desclassificado e o licitante subsequente convocado.

7.5. A aceitação da proposta fica condicionada à aprovação das especificações contidas nos documentos solicitados.

7.6. Examinada(s) a(s) proposta(s) classificada(s) em primeiro lugar, quanto ao objeto e valor, caberá ao pregoeiro decidir motivadamente a respeito da sua aceitabilidade.

7.7. **O pregoeiro realizará a aceitação da proposta para o grupo, sendo impossível aceitar parte dos itens.**

7.7.1. O preço ofertado final de cada item que integra o grupo não pode ser superior ao valor estimado para a respectiva contratação.

7.8. Em seguida, o pregoeiro verificará a habilitação do licitante conforme disposições do edital.

7.9. Constatado o atendimento pleno das exigências contidas no edital, o proponente será declarado vencedor.

7.10. Será desclassificada a proposta que:

7.10.1. não estiver em conformidade com os requisitos estabelecidos neste edital;

7.10.2. contenha vício insanável ou ilegalidade;

7.10.3. não apresente as especificações técnicas exigidas pelo Termo de Referência;

7.10.4. apresente preço final superior ao estimado, ou que apresente preço manifestamente inexequível.

7.11. Se a proposta for desclassificada ou se o licitante não atender às exigências habilitadoras, o pregoeiro examinará as propostas subsequentes, na ordem de classificação, até a obtenção de uma que atenda ao edital.

7.12. Será desconsiderada qualquer oferta de vantagem não prevista neste edital.

7.13. O pregoeiro, em qualquer fase do procedimento, poderá promover diligências julgadas necessárias à análise das propostas e da documentação, e os licitantes deverão atender às solicitações no prazo por ele estipulado, contado do recebimento da notificação.

7.14. Se um dos licitantes estiver impedido de participar em licitações ou tiver sido declarado inidôneo para licitar e contratar com a Administração Pública, será afastado do certame sem prejuízo das sanções legais cabíveis.

7.15. No julgamento da habilitação e das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos, nem sua validade jurídica, mediante despacho fundamentado registrado em ata e acessível a todos, e lhes atribuirá validade e eficácia para fins de habilitação e classificação.

7.16. **A(s) empresa(s) vencedora(s) do certame somente deverá(ão) encaminhar proposta(s), declarações ou quaisquer outros documentos se expressamente solicitado pelo pregoeiro, mediante notificação efetuada pelo canal de comunicação (*chat*), sob pena de serem descartados.**

7.17. O sistema eletrônico produzirá automaticamente ata circunstanciada da sessão pública imediatamente após seu encerramento, a qual ficará acessível no Portal de Compras do Governo Federal (www.comprasgovernamentais.gov.br) e nela serão registradas as ocorrências relevantes.

8. Requisitos de Habilitação dos Licitantes

8.1. A habilitação será verificada por meio do SICAF, nos documentos por ele abrangidos, podendo os licitantes deixar de apresentar os documentos de habilitação que já constem do referido Sistema de Cadastramento.

8.2. A habilitação no que tange à **regularidade fiscal** far-se-á com a verificação de que o licitante está em situação regular perante a Fazenda Nacional, a Seguridade Social e o Fundo de Garantia do Tempo de Serviço – FGTS, e as Fazendas Estaduais e Municipais, quando for o caso.

8.3. A **regularidade trabalhista** do licitante deverá ser comprovada mediante certidão negativa, provando a inexistência de débitos inadimplidos perante a Justiça do Trabalho, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n.º 5.452, de 1º de maio de 1943, a qual será emitida pelo Pregoeiro no sítio do TST durante a sessão pública.

8.4. Para comprovação da qualificação **econômico-financeira**, será exigido Índice de Liquidez Corrente (ILC) superior a um. Se o balanço patrimonial cadastrado no SICAF estiver vencido, o licitante deverá apresentar Balanço Patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, em que sejam nomeados os valores do ativo circulante (AC) e do passivo circulante (PC), de modo a extrair-se Índice de Liquidez Corrente (ILC) superior a um, vedada a substituição por balancetes ou balanços provisórios.

8.4.1. As empresas que apresentarem ILC igual ou menor do que um quando de sua habilitação, em vista dos riscos para a administração, deverão comprovar capital social no valor mínimo de dez por cento do valor da contratação resultante da licitação, admitida a atualização para a data de apresentação da proposta mediante índices oficiais.

8.4.2. Após 30 de abril, serão considerados válidos, para fins de habilitação, apenas os balanços patrimoniais do ano anterior, sendo que, se adotada a Escrituração Contábil Digital, as empresas vinculadas ao Sped só estarão obrigadas a apresentar o balanço do ano anterior após 31 de julho, conforme Instrução Normativa 1.950/2020 da Receita Federal do Brasil.

8.4.3. As empresas com menos de um exercício financeiro devem cumprir a exigência deste item mediante apresentação de Balanço de Abertura ou do último Balanço Patrimonial levantado, conforme o caso.

8.4.4. Não será exigido das microempresas ou das empresas de pequeno porte a apresentação do índice mencionado no item 8.4, ficando dispensadas de apresentar o balanço patrimonial do último exercício social, conforme previsto no artigo 3º, do Decreto nº 8.538/2015.

8.4.4.1. Neste caso, a qualificação econômico-financeira poderá ser comprovada por meio do contrato social, ou da certidão simplificada emitida pela junta comercial, demonstrando um capital social mínimo não inferior a 10% do valor total da proposta aceita.

8.5. A **qualificação técnica** será comprovada mediante apresentação de, pelo menos, um atestado de capacidade técnica compatível com o objeto desta licitação.

8.5.1. Entende-se por compatível, a prestação dos serviços que contemplem, pelo menos:

8.5.1.1. Fornecimento de solução de segurança da informação, composta de pelo menos um cluster de equipamento do tipo NGFW;

8.5.1.2. Prestação de serviço de suporte técnico para a solução de segurança;

8.5.1.3. Disponibilização de licenças e de atualização de assinatura;

8.5.1.4. Garantia.

8.5.2. Caso entenda necessário, o pregoeiro, por meio de diligência, poderá solicitar ao licitante a comprovação da legitimidade dos atestados apresentados, devendo o licitante disponibilizar todas as informações pertinentes, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços.

8.6. Disposições gerais sobre habilitação:

8.6.1. **Os licitantes que estiverem em situação regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF poderão deixar de apresentar os documentos referentes à HABILITAÇÃO JURÍDICA, QUALIFICAÇÃO ECONÔMICO-FINANCEIRA, REGULARIDADE FISCAL e TRABALHISTA.**

8.6.2. Os documentos exigidos para habilitação que não estejam contemplados no SICAF serão enviados nos termos do disposto no item 4.1.

8.6.3. Na hipótese de necessidade de envio de documentos complementares após o julgamento da proposta, estes deverão ser apresentados em formato digital, via sistema, no **prazo de duas horas** contado da solicitação do Pregoeiro.

8.6.3.1. Comprovada a impossibilidade de envio por meio da referida ferramenta, a critério do Pregoeiro, poderá ser utilizada outra forma de envio.

8.6.3.2. O prazo para envio poderá ser prorrogado por mais uma hora, a critério do Pregoeiro, desde que solicitado e justificado pelo interessado no chat da sessão pública ou por e-mail antes de expirado o prazo inicial estabelecido.

8.6.4. Para fins de habilitação, a verificação pelo órgão promotor do certame nos portais oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova.

8.6.5. Se a documentação de habilitação não estiver completa e correta, ou contrariar qualquer dispositivo deste edital, poderá o pregoeiro considerar o proponente inabilitado.

8.6.6. Caso o licitante seja inabilitado por irregularidade constatada quando da consulta no SICAF, e comprovar, exclusivamente mediante apresentação do Recibo de Solicitação de Serviço – RSS, nos termos do art. 37 da IN SLTI/MPOG n.º 02, de 11/10/2010, ter entregado a documentação à sua Unidade Cadastradora no prazo regulamentar, o pregoeiro suspenderá os trabalhos para proceder diligência, na forma estabelecida no § 3º do art. 43 da Lei n.º 8.666/1993.

8.6.7. Os documentos deverão ter validade expressa ou estabelecida em lei, admitidos como válidos, no caso de omissão, os emitidos a menos de noventa dias.

8.6.8. Não serão aceitos **protocolos de entrega** ou **solicitação de documento** em substituição aos documentos requeridos no presente edital.

8.6.9. Os documentos apresentados com a validade expirada, se não for falta sanável, acarretarão a inabilitação do proponente.

8.6.10. **Para as microempresas e empresas de pequeno porte, a comprovação da regularidade fiscal e trabalhista observará a disciplina estabelecida nos artigos 42 e 43 da Lei Complementar 123, de 14/12/06, regulamentados pelo art. 4º do Decreto 8.538, de 06/10/15, com as alterações trazidas pelas Leis Complementares 147/2014 e 155/2016.**

8.6.11. No ato de assinatura do contrato será exigida a comprovação das condições de habilitação consignadas neste edital, as quais deverão ser mantidas pela Contratada durante a vigência contratual.

9. Instruções e Normas para Impugnação do Edital e Interposição de Recursos

9.1. Em até **três dias úteis** antes da data fixada para abertura da sessão pública, qualquer pessoa poderá **impugnar** o ato convocatório do pregão eletrônico.

9.1.1. A impugnação não possui efeito suspensivo e caberá ao pregoeiro, auxiliado pelo setor responsável pela elaboração do edital e seus anexos, decidir sobre a impugnação no prazo de dois dias úteis da data do seu recebimento.

9.1.2. Acolhida a impugnação contra o ato convocatório, será definida e publicada nova data para realização do certame.

9.2. Os **pedidos de esclarecimento** referentes ao processo licitatório deverão ser enviados ao pregoeiro até **três dias úteis** anteriores à data fixada para abertura da sessão pública, exclusivamente por meio eletrônico via Internet (e-mail), para o endereço indicado na folha de rosto, em mensagens escritas que **não podem conter qualquer tipo de anexo**, nem serem encaminhados após as 19 horas do último dia do

prazo, sob pena de serem descartadas, **assim como as impugnações que não observarem as mesmas restrições de prazo, forma e conteúdo.**

9.2.1. Caberá ao pregoeiro, auxiliado pelo setor responsável pela elaboração do edital e seus anexos, decidir sobre os pedidos de esclarecimento no prazo de dois dias úteis da data do seu recebimento.

9.3. A formulação da proposta, sem impugnação tempestiva ao edital, implica a plena aceitação pelos interessados das condições nela estabelecidas.

9.4. Declarado o vencedor, qualquer licitante poderá manifestar sua intenção de recorrer ao final da sessão pública, imediata e motivadamente, em campo próprio do sistema, tendo três dias para apresentar as razões de recurso. Os demais licitantes ficam, desde logo, notificados a apresentar contrarrazões em igual prazo contado do término do prazo do recorrente, assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

9.5. O encaminhamento das razões de recurso, bem assim das contrarrazões, deverá ser efetuado somente por meio do sistema eletrônico.

9.6. O recurso contra decisão do Pregoeiro não terá efeito suspensivo.

9.7. A falta de manifestação imediata e motivada do licitante quanto à intenção de recorrer importará a decadência desse direito e o pregoeiro estará autorizado a adjudicar o objeto ao licitante declarado vencedor.

9.8. O acolhimento de recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento.

9.9. Se não reconsiderar sua decisão, o pregoeiro submeterá o recurso devidamente informado à consideração da autoridade competente que proferirá decisão definitiva antes da homologação do procedimento.

9.10. Os autos do processo administrativo eletrônico permanecerão com vista franqueada aos interessados, que deverão solicitá-la pelo e-mail cpl@tst.jus.br.

10. Prazos e Condições para Assinatura do Contrato

10.1. Após a homologação do resultado desta licitação, o TST convocará a empresa adjudicatária para assinatura do instrumento contratual, quando será exigida a comprovação das condições de habilitação consignadas no edital e, no caso das Microempresas e Empresas de Pequeno Porte optantes pelo Simples Nacional, deverá ser entregue declaração de que é regularmente inscrita neste sistema tributário, conforme inciso XI do art. 4º e modelo constante no anexo IV da Instrução Normativa RFB n.º 1.234, de 11 de janeiro de 2012.

10.1.1. O contrato deverá ser assinado, preferencialmente, por certificado digital emitido por Autoridade Certificadora referida na Medida Provisória 2.200-

2/2001, que instituiu a Infra-Estrutura de Chaves Públicas Brasileira-ICPBrasil, e enviado exclusivamente para o e-mail contratos@tst.jus.br.

10.1.2. Alternativamente à assinatura digital, o representante legal ou o procurador da adjudicatária poderá enviar e-mail para o endereço informado no item anterior para fins de ser estipulada outra forma de assinatura e envio do contrato, enquanto durar o período de funcionamento remoto das atividades do TST devido à pandemia de Coronavírus.

10.2. A convocação de que trata o item anterior deverá ser atendida no prazo máximo de dois dias úteis, prorrogável uma única vez a critério do TST, sob pena de decair o direito à contratação e de serem aplicadas as sanções previstas no item 18.3 deste edital.

10.2.1. O prazo tem início na data de envio do contrato, excluindo-se da contagem o dia do envio e incluindo-se o do vencimento.

10.2.2. As notificações ou convocações enviadas ao e-mail da licitante constante da proposta de preço ou de qualquer outro documento enviado na sessão pública do pregão eletrônico serão reputadas entregues, independente de confirmação de recebimento.

10.3. Não serão admitidos recursos, protestos, representações, ressalvas ou outra forma de discordância ou inconformismo a quaisquer tópicos do contrato que guardem absoluta conformidade com sua minuta, em expressão e substância.

10.4. Não será aceita apólice de seguro que contenha cláusula que exclua de cobertura prejuízos e demais penalidades causados ou relacionados a atos ou fatos violadores de normas de anticorrupção que tenham sido provocados exclusivamente pelo tomador ou seu representante, sem o concurso do segurado ou seu representante.

10.5. Ao assinar o instrumento contratual e retirar a nota de empenho, a Contratada obriga-se a prestar os serviços e entregar os produtos conforme especificações e condições contidas neste edital e na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital.

10.6. Quando o proponente vencedor não comprovar sua habilitação por ocasião da assinatura do contrato ou recusar-se a assiná-lo no prazo e condições estabelecidos, é facultado ao TST convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo, após comprovada a habilitação e feita a negociação, ou revogar a licitação independentemente das sanções previstas neste edital.

11. Vigência do Contrato

11.1. A vigência do contrato será da data da sua assinatura até cento e vinte dias após o recebimento definitivo do objeto.

12. Fiscalização da Execução Contratual

12.1. A execução do objeto deste pregão eletrônico será fiscalizada por um servidor, ou comissão de servidores, designados pela Administração, doravante denominado Fiscalização, com autoridade para exercer toda e qualquer ação de orientação geral durante a execução contratual.

12.2. São atribuições da Fiscalização, entre outras:

12.2.1. Acompanhar, fiscalizar e atestar a execução contratual, bem assim indicar as ocorrências verificadas;

12.2.2. Solicitar à Contratada e a seus prepostos ou obter da Administração todas as providências tempestivas necessárias ao bom andamento do contrato e anexar aos autos cópia dos documentos que comprovem essas solicitações;

12.2.3. Manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica;

12.2.4. Notificar a Contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto para que sejam adotadas as medidas corretivas necessárias;

12.2.5. Propor a aplicação de penalidades à Contratada e encaminhar à Coordenadoria de Material e Logística - CMLOG os documentos necessários à instrução de procedimentos para possível aplicação de sanções administrativas.

12.3. A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

13. Condições de Recebimento do Objeto da Licitação

13.1. O objeto da presente licitação, **relativamente aos itens 1 a 3**, será recebido das seguintes formas:

13.1.1. **Provisória,** mediante recibo, imediatamente após a entrega dos equipamentos e execução dos serviços, para efeito de posterior verificação de sua conformidade;

13.1.2. **Definitiva,** mediante recibo, em até dez dias úteis após o recebimento provisório e a verificação da perfeita execução das obrigações contratuais, ocasião em que se fará constar o atesto da nota fiscal.

13.2. O **item 4** (treinamento) será recebido da seguinte forma:

13.2.1. **Provisória,** mediante termo circunstanciado, imediatamente depois de efetuada a entrega do objeto, mediante a entrega também de lista de frequência dos participantes, para efeito de posterior verificação de sua conformidade;

13.2.2. **Definitiva,** mediante termo circunstanciado, em até dez dias úteis após o recebimento provisório e a verificação da perfeita execução das obrigações contratuais.

13.3. Os equipamentos entregues e os serviços prestados em desconformidade com o especificado no instrumento convocatório ou o indicado na proposta serão rejeitados parcial ou totalmente, conforme o caso, e a Contratada será notificada e obrigada a substituí-los ou refazê-los a suas expensas, no prazo contratual estabelecido, sob pena de incorrer em atraso quanto ao prazo de execução.

13.3.1. Essa notificação suspende os prazos de recebimento e de pagamento até que a irregularidade seja sanada.

13.4. Independentemente da aceitação, a Contratada garantirá a qualidade de cada produto fornecido e instalado e estará obrigada a repor aquele que apresentar defeito no prazo determinado pelo Contratante.

13.5. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança dos serviços prestados, nem a ético-profissional pela perfeita execução contratual, dentro dos limites estabelecidos pela lei.

14. Condições de Pagamento

14.1. O pagamento será efetuado em moeda corrente nacional, em até dez dias úteis após o recebimento definitivo, mediante apresentação da nota fiscal devidamente atestada pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

14.1.1.1. O pagamento dos itens 1 e 2 será efetuado após o recebimento definitivo da solução;

14.1.1.2. O pagamento dos itens 3 e 4 será efetuado após o recebimento definitivo dos serviços.

14.1.2. As notas fiscais e os documentos exigidos no edital para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Coordenadoria de Material e Logística do TST, situada no SAFS, quadra 8, conjunto A, bloco A, térreo, sala T18, CEP 70070-943, Brasília-DF, (61) 3043-4080.

14.1.3. A Nota Fiscal deverá corresponder ao objeto recebido e respectivos valores consignados na nota de empenho, e a Fiscalização, no caso de divergência, especialmente quando houver adimplemento parcial, deverá notificar a Contratada a substituí-la em até três dias úteis, com suspensão do prazo de pagamento.

14.2. A Contratada deverá entregar todos os produtos e prestar todos os serviços solicitados por meio da nota de empenho e ordem de serviço, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento total da obrigação.

14.3. A retenção dos tributos não será efetuada caso a Contratada apresente, no ato de assinatura do contrato ou entrega da nota de empenho, declaração de que é regularmente inscrita no Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte - Simples Nacional, conforme exigido no inciso XI do art. 4º e modelo constante no anexo IV da Instrução Normativa RFB n.º 1.234, de 11 de janeiro de 2012.

14.4. O Contratante pagará à Contratada a atualização monetária sobre o valor devido entre a data do adimplemento das obrigações contratuais e a do efetivo pagamento, excluídos os períodos de carência para recebimento definitivo e liquidação das despesas, previstos neste edital, e utilizará o índice publicado pela Fundação Getúlio Vargas que represente o menor valor acumulado no período, desde que a Contratada não tenha sido responsável, no todo ou em parte, pelo atraso no pagamento.

15. Reajustamento dos Preços

15.1. Os preços ofertados serão fixos e irreajustáveis.

16. Obrigações da Contratada

16.1. Executar os serviços e entregar os produtos objeto desta licitação na forma e em prazo não superior ao máximo estipulado neste edital.

16.2. Reparar, corrigir, remover e substituir, a suas expensas, as partes do objeto deste edital em que se verifiquem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços.

16.2.1. A Contratada deverá retirar o material ou componente recusado no momento da entrega do correto.

16.2.2. O Contratante não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo, podendo a Administração dar a destinação que julgar conveniente ao material abandonado em suas dependências.

16.3. Comunicar ao Contratante, por escrito, qualquer anormalidade referente à entrega dos produtos e à execução dos serviços, bem como atender prontamente às suas observações e exigências e prestar os esclarecimentos solicitados.

16.4. Atender prontamente as solicitações da fiscalização do contrato, inerentes ao objeto, sem qualquer ônus adicional para o Contratante.

16.5. Cumprir todos os requisitos descritos no edital, responsabilizando-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para o Contratante.

16.6. Respeitar o sistema de segurança do Contratante e fornecer todas as informações solicitadas por ele, relativas ao cumprimento do objeto.

16.7. Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

16.8. Guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do Contratante, sendo vedada, à Contratada, sua cessão, locação ou venda a terceiros.

16.9. Utilizar padrões definidos em conjunto com o Tribunal (nomenclaturas, metodologias, etc.).

16.10. Cumprir os prazos de execução descritos no Anexo I do Termo de Referência.

16.11. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do art. 57 da Lei nº 8.666/1993.

16.12. Fornecer, por ocasião da entrega do objeto, a documentação de suporte técnico e manutenção em garantia, contendo as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente, etc.).

16.13. Cumprir os requisitos de garantia, bem como os prazos de início de atendimento e de conclusão do reparo do equipamento, descritos no Anexo I do Termo de Referência anexo.

16.13.1. O fornecedor deverá assegurar a garantia dos equipamentos, seja por meio da rede mantida pelo próprio fabricante ou por meio de rede por ele credenciada, sendo, em todo caso, capaz de atender no local de entrega dos equipamentos com, no mínimo, um estabelecimento técnico.

16.13.2. O término do reparo do equipamento não poderá ultrapassar o prazo previsto; caso contrário, a Contratada deverá providenciar a colocação de equipamento equivalente ou de superior configuração, em perfeitas condições de uso, como backup, até que seja sanado o defeito do equipamento. O prazo máximo para o backup permanecer no Tribunal não deverá ser superior a 30 (trinta) dias, caracterizando, neste caso, a inexecução total da obrigação, punível com as sanções previstas no item 18.1.

16.14. Manter o Contratante informado quanto a eventuais mudanças de endereço, telefone e e-mail.

16.15. Manter, durante todo o período de execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas.

16.16. Responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, os quais não têm nenhum vínculo empregatício com o TST.

16.17. Responder, integralmente, por perdas e danos que vier a causar diretamente ao TST ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

16.18. A Contratada não será responsável:

16.18.1. Por qualquer perda ou dano resultante de caso fortuito ou força maior;

16.18.2. Por quaisquer obrigações, responsabilidades, trabalhos ou serviços não previstos neste edital.

16.19. O TST não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros, sejam fabricantes, representantes ou quaisquer outros.

17. Obrigações do TST

17.1. O TST, após a assinatura do contrato, compromete-se a:

17.1.1. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitir o acesso dos funcionários da Contratada às dependências do TST, relacionadas à execução do objeto deste edital;

17.1.2. Promover os pagamentos nas condições e dentro do prazo estipulado; e

17.1.3. Fornecer atestados de capacidade técnica, desde que atendidas às obrigações contratuais. Os requerimentos deverão ser protocolizados ou enviados por correspondência para o Protocolo Geral do TST, localizado no SAFS, quadra 08, conjunto A, bloco A, térreo, Brasília-DF, CEP 70.070-943.

18. Sanções para o Caso de Inadimplemento

18.1. Fundamentado no artigo 49 do Decreto n.º 10.024/2019, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 5 (cinco) anos, garantido o direito à ampla defesa, sem prejuízo das multas previstas neste edital e no contrato e das demais cominações legais, aquele que:

18.1.1. Não assinar o contrato;

18.1.2. Não entregar documentação exigida neste edital;

18.1.3. Apresentar documentação falsa;

18.1.4. Causar o atraso na execução do objeto;

18.1.5. Não mantiver a proposta;

18.1.6. Falhar ou fraudar na execução contratual;

18.1.7. Comportar-se de modo inidôneo;

18.1.8. Declarar informações falsas;

18.1.9. Cometer fraude fiscal.

18.2. O atraso injustificado na execução contratual implicará multa correspondente a 0,5% (cinco décimos por cento) por dia de atraso, calculada sobre o valor do objeto em atraso, até o limite de 15% (quinze por cento) do respectivo valor total.

18.2.1. Nessa hipótese, o atraso injustificado por período superior a 30 (trinta) dias caracterizará o descumprimento total da obrigação, punível com a sanção prevista no item 18.1 deste edital, como também a inexecução total contratual.

18.3. No caso de atraso no cumprimento do prazo de assinatura do contrato, assinalado no item 10.2 deste edital, será aplicada multa de 0,5% (cinco décimos por cento) ao dia sobre o valor total contratado, até o limite de 15% (quinze por cento).

18.4. Durante a execução do contrato, caso existam ocorrências que ultrapassem os níveis de tolerância informados nos requisitos de prazo do Anexo I do Termo de Referência, serão aplicadas multas, detalhadas a seguir:

18.4.1. 1% (um por cento) ao dia sobre o valor referente ao respectivo item, no caso de atraso injustificado para a entrega dos equipamentos e do software de gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;

18.4.2. 1% (um por cento) ao dia sobre o valor referente aos itens a serem instalados, no caso de atraso injustificado para conclusão do Serviço de Instalação dos Equipamentos e do Software de Gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;

18.4.2.1. Para o item 1, 2% (dois por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 1 (CRÍTICA);

18.4.2.2. Para o item 1, 1% (um por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos

estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 2 (ALTA);

18.4.2.3. Para o item 1, 0,5% (meio por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (MÉDIA);

18.4.2.4. Para o item 1, 0,25% (vinte e cinco décimos percentuais) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (BAIXA).

18.5. Poderão ser aplicadas subsidiariamente as sanções de advertência, suspensão e declaração de inidoneidade previstas nos artigos 86 e 87 da Lei n.º 8.666/93.

18.6. A penalidade de multa prevista nos itens 18.2 a 18.4 poderá ser substituída pela penalidade de advertência, tendo em vista as circunstâncias da execução contratual, garantida a prévia defesa, na forma da lei.

18.7. As multas porventura aplicadas serão descontadas dos pagamentos devidos pelo TST ou cobradas diretamente da empresa, amigável ou judicialmente, e poderão ser aplicadas cumulativamente com as demais sanções previstas neste tópico.

18.8. As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

18.9. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei 8.666/93, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

18.9.1. Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, quadra 08, conjunto A, bloco A, térreo, sala T-18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4096, e-mail: sgcon@tst.jus.br.

18.9.2. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

19. Generalidades

19.1. O CNPJ do TST é 00.509.968/0001-48 e a UASG é 080001.

19.2. Esta licitação poderá ser revogada total ou parcialmente, sem que caiba indenização aos licitantes em consequência do ato, nos termos do art. 50 do Decreto 10.024/2019.

19.3. No curso da contratação, é admitida a fusão, cisão ou incorporação da empresa, bem assim sua alteração social, modificação da finalidade ou da estrutura, desde que não prejudique a execução contratual, cabendo à Administração decidir pelo prosseguimento ou rescisão contratual.

19.4. Em consonância com a Resolução 7, de 18 de outubro de 2005, do Conselho Nacional da Justiça, constante do Anexo I, é vedada a contratação de empresas 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.

19.4.1. A vedação constante no item anterior se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

19.5. É de responsabilidade do Proponente o conhecimento das características dos serviços e produtos relacionados no objeto desta licitação.

19.6. Em caso de discrepância entre o Edital, seus anexos e os dados incluídos no sistema Comprasnet, prevalecerá a redação do instrumento convocatório.

19.7. Quaisquer outros elementos necessários ao perfeito entendimento deste edital poderão ser obtidos na Coordenadoria de Licitações e Contratos, exclusivamente pelo endereço eletrônico cpl@tst.jus.br.

19.8. Esta licitação poderá ser acompanhada pelos portais www.tst.jus.br e www.comprasgovernamentais.gov.br, onde são divulgados os prazos, consultas e demais informações do certame.

ANEXO I

RESOLUÇÃO CNJ Nº 7, DE 18 DE OUTUBRO DE 2005

Art. 1° É vedada a prática de nepotismo no âmbito de todos os órgãos do Poder Judiciário, sendo nulos os atos assim caracterizados.

Art. 2° Constituem práticas de nepotismo, dentre outras:

I - o exercício de cargo de provimento em comissão ou de função gratificada, no âmbito da jurisdição de cada Tribunal ou Juízo, por cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados;

II - o exercício, em Tribunais ou Juízos diversos, de cargos de provimento em comissão, ou de funções gratificadas, por cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de dois ou mais magistrados, ou de servidores investidos em cargos de direção ou de assessoramento, em circunstâncias que caracterizem ajuste para burlar a regra do inciso anterior mediante reciprocidade nas nomeações ou designações;

III - o exercício de cargo de provimento em comissão ou de função gratificada, no âmbito da jurisdição de cada Tribunal ou Juízo, por cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de qualquer servidor investido em cargo de direção ou de assessoramento;

IV - a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público, de cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados, bem como de qualquer servidor investido em cargo de direção ou de assessoramento;

V - a contratação, em casos excepcionais de dispensa ou inexigibilidade de licitação, de pessoa jurídica da qual sejam sócios cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, dos respectivos membros ou juízes vinculados, ou servidor investido em cargo de direção e de assessoramento; (Redação dada pela Resolução nº 229, de 22.06.16)

VI - a contratação, 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. (Incluído pela Resolução nº 229, de 22.06.16)

§ 1º Ficam excepcionadas, nas hipóteses dos incisos I, II e III deste artigo, as nomeações ou designações de servidores ocupantes de cargo de provimento efetivo das carreiras judiciárias, admitidos por concurso público, observada a compatibilidade do grau de escolaridade do cargo de origem, a qualificação profissional do servidor e a complexidade inerente ao cargo em comissão a ser exercido, e que o outro servidor também seja titular de cargo de provimento efetivo das carreiras judiciárias, vedada, em qualquer caso a nomeação ou designação para servir subordinado ao magistrado ou servidor determinante da incompatibilidade. (Redação dada pela Resolução nº 181, de 17.10.13)

§ 2° A vedação constante do inciso IV deste artigo não se aplica quando a contratação por tempo determinado para atender a necessidade temporária de excepcional interesse público houver sido precedida de regular processo seletivo, em cumprimento de preceito legal.

§ 3º A vedação constante do inciso VI deste artigo se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização. (Incluído pela Resolução nº 229, de 22.06.16)

§ 4º A contratação de empresa pertencente a parente de magistrado ou servidor não abrangido pelas hipóteses expressas de nepotismo poderá ser vedada pelo tribunal, quando, no caso concreto, identificar risco potencial de contaminação do processo licitatório. (Incluído pela Resolução nº 229, de 22.06.16)

Art. 3º É vedada a manutenção, aditamento ou prorrogação de contrato de prestação de serviços com empresa que venha a contratar empregados que sejam cônjuges, companheiros ou parentes em linha reta, colateral ou por afinidade, até o terceiro grau, inclusive, de ocupantes de cargos de direção e de assessoramento, de membros ou juízes vinculados ao respectivo Tribunal contratante, devendo tal condição constar expressamente dos editais de licitação. (Redação dada pela Resolução n° 9, de 06.12.05)

Art. 4° O nomeado ou designado, antes da posse, declarará por escrito não ter relação familiar ou de parentesco que importe prática vedada na forma do artigo 2°.

Art. 5° Os Presidentes dos Tribunais, dentro do prazo de noventa dias, contado da publicação deste ato, promoverão a exoneração dos atuais ocupantes de cargos de provimento em comissão e de funções gratificadas, nas situações previstas no art. 2°, comunicando a este Conselho.

Parágrafo único Os atos de exoneração produzirão efeitos a contar de suas respectivas publicações.

Art. 6° O Conselho Nacional de Justiça, em cento e oitenta dias, com base nas informações colhidas pela Comissão de Estatística, analisará a relação entre cargos de provimento efetivo e cargos de provimento em comissão, em todos os Tribunais, visando à elaboração de políticas que privilegiem mecanismos de acesso ao serviço público baseados em processos objetivos de aferição de mérito.

Art. 7° Esta Resolução entra em vigor na data de sua publicação.

<table>
<tr><th colspan="3">Relação familiar</th></tr>
<tr><td colspan="3">I - Cônjuge ou companheiro.</td></tr>
<tr><td colspan="3">II - Relação de parentesco até o 3º grau, inclusive.</td></tr>
<tr><td colspan="3">II.1 - Parentesco natural e civil.</td></tr>
<tr><td rowspan="2">Linha reta</td><td>Ascendente</td><td>a) pais - 1º grau
b) avós - 2º grau
c) bisavós - 3º grau</td></tr>
<tr><td>Descendente</td><td>a) filhos - 1º grau
b) netos - 2º grau
c) bisnetos - 3º grau</td></tr>
<tr><td colspan="2">Linha colateral</td><td>a) irmãos - 2º grau
b) tios e sobrinhos – 3º grau</td></tr>
<tr><td colspan="3">II.2 - Parentesco por afinidade</td></tr>
<tr><td rowspan="2">Linha reta</td><td>Ascendente</td><td>a) sogros (pais do cônjuge ou companheiro) - 1º grau
b) padrasto ou madrasta - 1º grau
c) padrasto ou madrasta do cônjuge ou companheiro - 1º grau
d) avós do cônjuge ou companheiro - 2º grau
e) bisavós do cônjuge ou companheiro - 3º grau</td></tr>
<tr><td>Descendente</td><td>a) genro ou nora (cônjuge ou companheiro dos filhos) - 1º grau
b) enteados (filhos do cônjuge ou companheiro) - 1º grau
c) filhos dos enteados (netos do cônjuge ou companheiro) - 2º grau
d) netos dos enteados (bisnetos do cônjuge ou companheiro) - 3º grau</td></tr>
<tr><td colspan="2">Linha colateral</td><td>a) cunhados - 2º grau
b) tios e sobrinhos do cônjuge ou companheiro - 3º grau</td></tr>
</table>

ANEXO II

DECLARAÇÃO

Identificação da Empresa:

Razão Social:
CNPJ:
Endereço:
Telefone:

Declaro, para fins de participação no Pregão Eletrônico n.º 031/2020, não haver no quadro societário da empresa identificada acima 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 do Tribunal Superior do Trabalho situadas na linha hierárquica da área encarregada da licitação.

A presente Declaração abrange um período de seis meses anteriores a esta data.

Local e data

_____

Representante da empresa

ANEXO III

DECLARAÇÃO

Identificação da Empresa:

Razão Social:
CNPJ:
Endereço:
Telefone:

Na condição de sócio(s) da empresa identificada acima, para fins de contratação decorrente do Pregão Eletrônico n.º 031/2020 declaro(amos) não incorrer na vedação do inciso VI do art. 2º da Resolução CNJ 7/2005, acrescentado pela Resolução CNJ 229/2016.

A presente Declaração abrange um período de seis meses anteriores a esta data.

Local e data

_____

Sócio 1

_____

Sócio 2

_____

Sócio 3

1. Definição do Objeto

1.1 Aquisição de solução de *firewall*.

1.2 Solução de segurança para redes de dados do tipo *Next Generation Firewall* de alta disponibilidade, compreendendo: sistema de detecção e prevenção de intrusão do TIPO IPS/IDS, gerenciamento centralizado e integrado, controle de ameaças, filtro de URL, controle de aplicação, suporte e garantia do fabricante, assinaturas de proteção e suporte técnico em repositório mundial do fabricante, suporte técnico do fabricante local e/ou remoto, incluindo serviços de instalação e treinamento.

Grupo	Item	Especificação	Unidade	Qtde.
01	01	*Cluster Firewall* NGFW	Equipamento	01
	02	Sistema de Gerenciamento – *Next Generation Security Management*	Un.	01
	03	Serviço de Instalação e Configuração	Serviço	01
	04	Treinamento especializado para 5 (cinco) alunos	Turma	01
Classificação do objeto: Equipamento de TIC - Ativos de Rede - 3.44.90.52.37				
Código do SIGEO: 151012020000172				
Código CATMAT/CATSER: 320365				

2. Fundamentação da Contratação

2.1 Motivação da Contratação

Atualmente o Tribunal Superior do Trabalho possui dois conjuntos de equipamentos de *Firewall*/IPS, que funcionam como um único *cluster*. Estes equipamentos foram adquiridos por meio da Ata de Registro de Preços PE-026/2012 do TST, com recursos descentralizados pelo CSJT e fornecem solução de alta disponibilidade para equipamento de segurança para redes de dados do tipo *Firewall*, com Sistema de Detecção e Prevenção de Intrusão do tipo IPS/IDS, padronizada para toda a JT e são utilizados para prover segurança ente a Internet e a Rede DMZ. Entretanto o fabricante Cisco Systems descontinuou a comercialização desses equipamentos em outubro de 2017.

A prestação jurisdicional na Justiça do Trabalho depende diretamente dos serviços de TIC que sustentam os sistemas informatizados do TST. Para sustentar o funcionamento dos sistemas são necessários vários tipos de redes de comunicação, entre elas a Internet, as redes locais dentro das dependências do TST (redes LAN), as redes privadas amplas, que conectam aos Tribunais Regionais do Trabalho, através da VPN, bem como as redes metropolitanas, que conectam as unidades dentro de uma área urbana (redes MAN). Toda a segurança dos dados que circulam entre todas as redes de dados do Tribunal, nos seus diferentes níveis de interligações, é promovida pelo equipamento *Firewall*, tornando este equipamento imprescindível para o negócio do Tribunal.

Atualmente o Tribunal Superior do Trabalho vem protegendo suas redes por meio de equipamentos *Firewall* atuando na interpretação e filtragem de dados na camada 3 do protocolo IP (camada de rede do modelo OSI). Contudo, o processo de modernização da infraestrutura de TIC, a ampliação do uso das redes de comunicação e o aprimoramento das técnicas de ataques contra as instituições que disponibilizam serviços de informática trazem a necessidade do fortalecimento da segurança da informação na Justiça do Trabalho e do estabelecimento de estratégia corporativa para prover os mais altos níveis de proteção às informações e sistemas.

Visando a garantir melhores condições de segurança das informações, com vistas à integridade dos processos eletrônicos judiciais e administrativos, faz-se necessário a implantação de soluções que atuem no controle e segurança das informações, nas camadas de rede mais avançadas, em nível de aplicação (camada 7), de modo a minimizar os riscos de exploração de possíveis ameaças e permitam, por meio de alarmes e controles, uma rápida resposta do Tribunal em caso de incidentes de segurança.

Para o contexto apresentado desponta como imprescindível a manutenção de solução de *Firewall* atualizada aos atuais padrões de mercado, com recursos de alta disponibilidade para sustentar o funcionamento institucional da Justiça do Trabalho.

2.2 Objetivos a serem alcançados

Dentre os objetivos a serem alcançados, destaca-se a manutenção e melhoria do nível de segurança atualmente em funcionamento no Tribunal Superior do Trabalho, de maneira a garantir da integridade e segurança do ambiente computacional da Corte e dos serviços de Tecnologia da Informação oferecidos pela SETIN.

Além disso, espera-se com a pretendida contratação:

- Garantir o nível de segurança dos serviços prestados pelo TST;
- Manter a conexão entre o TST e os TRTs através da conexão VPN;
- Manter equipamentos em garantia, suportados pelo fabricante, atualizados em sua última versão disponível;
- Obter o suporte técnico em caso de falha e/ou dúvidas, aumentando a segurança da rede do Tribunal.
- Garantir a disponibilidade dos serviços hospedados no *site* principal e no *site* de contingência.

2.3 Benefícios diretos e indiretos resultantes da contratação

Como citado anteriormente um dos componentes mais importantes de segurança da informação é a solução de *firewall*, objeto desta contratação, que possibilitará entre outras ações: o controle do tráfego de dados, proteção à rede do TST, monitoramento das conexões de entrada e saída, bloqueio de ameaças, conectividade entre o TST e os Regionais através de VPN.

Além disso, este dispositivo de segurança permite gerenciamento centralizado, diminuindo a complexidade de sua gerência e tornando mais simples auditorias, caso ocorram incidentes de segurança.

Com a aquisição de *firewall* do tipo NGFW (*Next Generation Firewall*) será possível detectar e bloquear ataques sofisticados, pois esse equipamento permite reforçar políticas de segurança na camada de aplicação, camada 7 no modelo OSI. A nova solução, em pleno funcionamento, com garantia e suporte do fornecedor, fará com que eventuais problemas tenham o menor impacto possível para a prestação jurisdicional.

Firewall do tipo NGFW integram 3 recursos chaves, que são a capacidade de *firewall*, sistema de prevenção de intrusão (IPS) e o controle de aplicação. Além do já exposto, a contratação da solução de segurança vai além da aquisição de equipamentos. É uma busca por uma solução que melhore a maturidade em segurança de rede do TST.

2.4 Alinhamento entre a contratação e os planos estratégicos do TST e planos estratégicos de Tecnologia da Informação

Consta no Plano de Contratações de STIC para o exercício de 2020 da Secretaria de Tecnologia da Informação do TST a **Ação Orçamentária 2020-AO-007**, com valor estimado de **R$ 1.200.000,00** (um milhão e duzentos mil reais).

2.5 Referência aos Estudos Preliminares de STIC realizados

Os estudos técnicos preliminares estão acostados no processo.

2.6 Relação entre a demanda prevista e a quantidade de cada item

Segue abaixo tabelas com os quantitativos para atender ao TST:

Descrição	Qtd
Cluster Firewall NGFW	1
Sistema de Gerenciamento – *Next Generation Security Management*	1
Serviço de Instalação e Configuração	1
Treinamento especializado para 5 (cinco) alunos	1

Tabela 1 – Quantitativo para solução de *Firewall* NG

Este é o quantitativo mínimo para a solução. É necessário um cluster por redundância, conforme descrito neste Estudo. Também é necessário um software para gerenciamento da solução, bem como um serviço de instalação e um treinamento da equipe.

2.7 Soluções similares disponíveis em outros órgãos e no Portal do Software Público Brasileiro

Não há solução disponível no Portal do *Software* Público Brasileiro.

2.8 Análise do mercado de Tecnologia da Informação e Comunicação

Foi feito uma análise de todo o mercado nos estudos técnicos preliminares da contratação.

O novo equipamento a ser contratado necessita ter sua capacidade compatível com o desempenho da rede atual e, ainda, com possível *upgrade* da rede que pode ocorrer nos próximos 5 anos (vigência da garantia solicitada), pois a rede atual já está preparada para funcionar com 25/100 Gbps, sendo o *upgrade* relativamente simples e com baixo custo.

Todos os requisitos tiveram como base os recursos e parâmetros oferecidos pelos equipamentos atuais adequados à velocidade da nova rede no datacenter, quando necessário.

Dentro deste contexto, levantamos as seguintes alternativas relacionadas à manutenção do serviço de filtro de acesso às redes corporativas:

Solução 1: Abandonar os equipamentos que hoje se encontram em operação e implantar *software* mantido pela comunidade com licença de uso aberta (*software* livre) para funcionar como *Firewall* e IPS.

Solução 2: Substituir os equipamentos hoje em funcionamento por solução mais completa de sistema de *firewall* com *IPS* em camada 7.

Solução 3: Manter os equipamentos atuais em operação contratando suporte para o equipamento *firewall* e efetuando *upgrade* da solução IPS, transformando o conjunto em um *firewall* camada 7 de nova geração – NG.

Para realizar a comparação, elaboramos o quadro abaixo como forma de resumir as questões levantadas.

ITENS ANALISADOS	SOLUÇÃO		
	1 (*software* livre)	3 (novo camada7)	5 (manter atual com *upgrade*)
Provável menor investimento?	Sim	Não	Não
Baixa complexidade do gerenciamento?	Não	Sim	Sim
Atualiza automaticamente a base de dados de *malware*?	Não	Sim	Sim
Possui banco de dados mundial para atualização automática de informações sobre códigos maliciosos?	Não	Sim	Sim
Confiabilidade associada a imagem de fabricante mundial?	Não	Sim	Sim
Permite dimensionamento de acordo com a necessidade do TST?	Não	Sim	Sim
Usa recursos computacionais dedicados, ou seja, não interfere nos recursos já alocados para outros sistemas do TST?	Não	Sim/Não[1]	Sim
Possui portfólio de clientes de porte semelhante ao do TST?	Sim	Sim	Sim
Necessita migração (troca) de solução?	Não	Sim	Sim
Necessita novo treinamento da equipe?	Sim	Sim	Sim
Mantém padrão de *Firewall* e *IPS* para a JT?	Não	Não	Não
Possui mais de um fabricante disponível?	Sim	Sim	Não
Preserva o investimento já realizado pela JT?	Não	Não	Sim
Necessita de troca de tecnologia?	Sim	Sim	Sim
Menor risco de invasão das redes lógicas?	Não	Sim	Sim

Tabela 2 – Quadro resumo do comparativo entre as possíveis soluções

1 Pode ser contratada solução baseada apenas em *software* ou *hardware* dedicado com *software*.
2 Caso seja contratada a mesma fabricante da solução camada 3, para a solução camada 7, não será preciso migração, treinamento, manterá o padrão e preservará o investimento.

Diferentemente de um modelo tradicional de *firewall* que faz controle de IP de origem/destino, porta de origem/destino e *flags* somente, um *Next Generation Firewall*-NGFW vai além, com análises mais profundas no pacote que é trafegado por ele.

Por exemplo, em um NGFW é possível analisar se um *download* que está sendo feito contém algum tipo de ameaça, como um *ransomware* ou outro *malware* qualquer, conhecido (que já tenha assinatura) ou desconhecido (*Zero Day*).

O NGFW agrega função de IPS, ou seja, enxergam dentro dos pacotes de rede se existe alguém mal intencionado tentando explorar vulnerabilidade em algum serviço que roda na infraestrutura do TST, por exemplo, apache, RDP, Oracle, JBoss, SSH, SQL Server e muitos outros.

Outra funcionalidade extremamente importante é a de URL *Filtering*, onde é possível controlar o acesso a milhares de *sites* não desejados, com base nas políticas do TST, e evitar incidentes de segurança, uso indevido dos recursos de rede da empresa (uso de *torrents* e *Streaming*, por exemplo) e outras situações não desejadas. Além da possibilidade de prevenção contra vazamento de dados (DLP) sensíveis para o negócio.

Cabe destacar, ainda, o recurso conhecido com *Sandbox* que é usado, dentre outras, para quarentenar ameaças não conhecidas que explorem vulnerabilidades não reportadas. Devido aos *malwares* hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com velocidade que suas variações são criadas, a solução deve possuir, dentre outras, funcionalidades para análise de *malware* não conhecidos, *Zero-Day*.

Desta forma a solução 2 é a mais adequada.

2.9 Natureza do objeto a ser contratado

Trata-se de aquisição de solução de segurança para redes de dados, mais especificamente hardware (equipamento) e software, bem como serviço de instalação, de suporte técnico e garantia do fabricante local e/ou remoto e treinamento de equipe técnica. Seus padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado. Portanto, a natureza do objeto a ser contratado é de bem/serviço comum.

2.10 Justificativas para o parcelamento ou não da solução

Por se tratar de um único conjunto de equipamentos, não é tecnicamente possível o parcelamento do objeto.

2.11 Forma de adjudicação do objeto

Os itens 1, 2 e 3 do objeto possuem uma certa dependência técnica entre si, de forma que é bastante recomendável ser adjudicado a uma única empresa. O sistema de gerenciamento é do mesmo fabricante que o sistema de hardware. E a instalação e configuração é justamente o serviço a se feito com o hardware e sistema de gerenciamento. Portanto, sugerimos fortemente que os três primeiros itens sejam adjudicados a uma única empresa.

Quanto ao treinamento, item 4, é possível ser adjudicado a outra empresa. Porém, a equipe técnica não recomenda, pois experiência passada na aquisição de outros objetos relevantes para o Tribunal revelou que há riscos em se fazer desta forma, como, por exemplo, o risco de não haver treinamento em tempo hábil (por falta de turmas, por

licitação deserta) e, considerando que o objeto desta licitação é extremamente crítico para o funcionamento da rede do Tribunal, a equipe recomenda que o treinamento seja também inserido no grupo anterior (itens 1, 2 e 3).

Além disso, boa parte do treinamento é instalação e configuração do equipamento e do sistema de gerenciamento. Isto é, bastante tempo é investido por técnicos da contratada configurando o sistema, como regras de filtragem, e sendo a mesma equipe da contratada há um ganho significativo para a aquisição de treinamento no mesmo grupo.

Porrtanto, concluímos que a adjudicação do objeto será global, de forma que os produtos formem um grupo único, compatíveis em marca e modelo e projeto, incluindo no grupo o treinamento.

2.12 Modalidade e tipo de licitação

O regime de contratação proposto é de Licitação por Pregão Eletrônico, com amparo na Lei nº 10.520/2002, regulamentada pelo Decreto nº 10.024/2019, combinados com o Decreto nº 3.555/2000 e com a Lei nº 8.666/93.

2.13 Impacto ambiental decorrente da contratação

Não haverá impacto ambiental decorrente da contratação. O equipamento atual poderá ser doado.

3. Modelo de execução e gestão do contrato

3.1 Deveres e responsabilidades do Contratante

3.1.1 Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações contratuais, inclusive permitir o livre acesso dos técnicos da Contratada às dependências do Contratante relacionadas à execução do contrato.

3.1.2 Promover os pagamentos em moeda corrente nacional, mediante depósito na conta bancária indicada pela Contratada, após o ateste da Nota Fiscal.

3.1.3 Fornecer atestados de capacidade técnica quando solicitado, desde que atendidas às obrigações contratuais.

3.1.4 Após a assinatura do contrato, o Contratante designará, formalmente, servidor ou comissão de servidores para exercerem o acompanhamento e fiscalização da execução contratual.

3.2 Deveres e responsabilidades da Contratada

3.2.1 Entregar o objeto e executar os serviços descritos no contrato nos prazos máximos nele determinados.

3.2.2 Atender prontamente as solicitações da fiscalização do contrato, inerentes ao objeto, sem qualquer ônus adicional para o órgão Contratante.

3.2.3 Cumprir todos os requisitos descritos no contrato, responsabilizando-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para o Contratante.

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

3.2.5 Responder pelas despesas relativas a encargos trabalhistas, seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, uma vez inexistir, no caso, vínculo empregatício deles com o Contratante.

3.2.6 Responder integralmente por perdas e danos que vier a causar ao Contratante ou a terceiros em razão de ação ou omissão dolosa ou culposa, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

3.2.7 Respeitar o sistema de segurança do Contratante e fornecer todas as informações solicitadas por ele, relativas ao cumprimento do objeto.

3.2.8 Acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades.

3.2.9 Guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do Contratante, sendo vedada, à Contratada, sua cessão, locação ou venda a terceiros.

3.2.10 Utilizar padrões definidos em conjunto com o Tribunal (nomenclaturas, metodologias, etc.).

3.2.11 Comprovar a quitação dos tributos de importação referentes aos produtos, conforme disposto no Decreto nº 7.174/2010, art. 3º, inc. III, da seguinte forma:

3.2.11.1 Caso os produtos entregues sejam importados e a Contratada for a importadora, a comprovação poderá ser feita por meio da apresentação dos seguintes documentos, sob pena de rescisão contratual e multa:

a) Comprovante de Importação emitido no Siscomex quando a Declaração de Importação – DI, é desembaraçada;

b) Última versão do extrato da Declaração de Importação.

3.2.11.1.1 Os bens fornecidos devem estar descritos na DI de forma a permitir a identificação precisa, constando marca, modelo e, se possível, nº de série.

3.2.11.2 Caso o produto entregue não seja importado deverá ser apresentada, no momento da entrega, uma declaração da Contratada atestando essa situação.

3.2.11.2.1 A declaração deverá ser apresentada mesmo para as empresas que participaram da licitação utilizando-se da preferência de que trata o art. 3º da Lei 8.248/91.

3.2.11.3 Caso o produto entregue seja importado, mas se a Contratada não for a titular da obrigação tributária correspondente, a contratada deverá comprovar, no momento da entrega, a aquisição do produto importado pelo contratado não importador, junto ao seu fornecedor, de modo a

afastar sua responsabilidade pelos tributos de importação, considerando não ser sujeito passivo tributário.

3.3 Especificação técnica do objeto

Especificação técnica detalhada do objeto está presente no Anexo I deste Termo de Referência.

3.4 Prazos de execução

3.4.1 O prazo para a entrega do objeto será de 60 (sessenta) dias corridos, a contar da assinatura do contrato ou do recebimento da nota de empenho pela Contratada, quando não houver instrumento contratual.

3.4.2 O endereço para entrega do objeto é: Coordenadoria de Infraestrutura Tecnológica, Tribunal Superior do Trabalho, SAFS, Quadra 8, Conjunto A, Bloco A, Sala 232, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4474.

3.4.3 Na contagem dos prazos previstos neste documento, excluir-se-á o dia de início e incluir-se-á o dia do vencimento. Só se iniciam e vencem os prazos em dias úteis e de expediente no Tribunal Superior do Trabalho.

3.4.4 Serão considerados injustificados os atrasos não comunicados tempestivamente e indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

3.4.5 Havendo pedido de prorrogação do prazo de entrega, este somente será concedido nas hipóteses previstas no Art. 57, §1°, da Lei nº 8.666/93, em caráter excepcional e sem efeito suspensivo, e deverá ser encaminhado por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

3.4.6 Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, Quadra 8, Conjunto A, Bloco A, Sala 18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4165, (061) 3043-4096, e-mail: sgcon@tst.jus.br.

3.4.7 Em casos excepcionais, autorizados pelo Contratante, o documento comprobatório do alegado poderá acompanhar a entrega do produto.

3.5 Garantia on-site do objeto

3.5.1 O prazo de garantia para todos os equipamentos do objeto será de 60 (sessenta) meses e será contado a partir do Recebimento Definitivo lavrado pela Contratante.

3.5.2 Os requisitos de garantia estão especificados no anexo I deste Termo de Referência.

3.5.3 Os prazos de início de atendimento e de conclusão do reparo do equipamento estão especificados nos requisitos técnicos de prazo – anexo I.

3.5.4 O fornecedor deverá assegurar a garantia dos equipamentos, seja por meio da rede mantida pelo próprio fabricante ou por meio de rede por ele credenciada,

sendo, em todo caso, capaz de atender no local de entrega dos equipamentos com, no mínimo, um estabelecimento técnico.

3.5.5 O término do reparo do equipamento não poderá ultrapassar o prazo previsto; caso contrário, a Contratada deverá providenciar a colocação de equipamento equivalente ou de superior configuração, em perfeitas condições de uso, como *backup*, até que seja sanado o defeito do equipamento. O prazo máximo para o *backup* permanecer no Tribunal não deverá ser superior a 30 (trinta) dias, caracterizando, neste caso, a inexecução total da obrigação, punível com as sanções previstas nos itens **3.11.2.3** e **3.11.2.4**.

3.6 Proposta Técnica

3.6.1 A licitante deverá apresentar Proposta Técnica, contendo a descrição detalhada do objeto ofertado, devendo estar de acordo com as quantidades, especificações técnicas e condições estabelecidas;

3.6.2 Deverá ser fornecida pela licitante uma tabela com o número das páginas de sua proposta na qual contenha a comprovação do atendimento dos requisitos exigidos;

3.6.3 Apresentar na proposta a indicação detalhada do equipamento ofertado citando a marca, modelo, tipo e fabricante;

3.6.4 A tabela de comprovação técnica é parte obrigatória da proposta comercial e deve ser apresentada conforme modelo abaixo. É necessária a especificação de TODOS os itens contidos neste Termo de Referência e no Edital e a apresentação da documentação comprobatória com indicação da página e com informações das funcionalidades e características exigidas, grifadas. Salienta-se que todos os itens da tabela devem ser devidamente preenchidos.

Nº Requisito no TR	Descrição da característica ou funcionalidade exigida	Documento do fabricante (nome)	Página(s)	Atende ao Requisito (sim/não)
R.HS1	.....	.....	.....	.....

3.6.5 Serão considerados documentos oficiais para comprovação técnica: catálogos, *folders*, prospectos e manuais;

3.6.6 Para os documentos do fabricante, é mandatório a comprovação que se trata de documento oficial fornecido pelo fabricante ao mercado, sendo comprovação suficiente desse requisito o *link* para o acesso ao documento no site do fabricante;

3.6.7 Havendo divergência entra as características técnicas descritas na proposta da licitante e as disponibilizadas pelo fabricante, prevalecerão os informes do fabricante, salvo os casos específicos em que o licitante esclareça os motivos da divergência e que sejam aceitos pelo TST;

3.6.8 Os documentos técnicos fornecidos que não apresentarem numeração de página deverão ser numerados manualmente de forma visível pela Licitante, no canto inferior direito;

3.6.9 Além da indicação da página da documentação fornecida na qual se encontra a comprovação de cada funcionalidade ou característica técnica exigida

para cada item, a correspondente comprovação deverá ser necessariamente grifada ou destacada com marca texto;

3.6.10 A CONTRATADA deverá arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do art. 57 da Lei nº 8.666/1993;

3.7 Habilitação Técnica

3.7.1 Para comprovação de que a empresa licitante possui capacitação técnica e experiência no fornecimento de solução correlata ao do objeto deste Termo de Referência, a empresa deverá, nos termos do Art. 30, parágrafo 1º, da Lei 8.666/93, juntamente com a documentação de habilitação necessária, comprovar aptidão para o desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto desta licitação, por meio da apresentação de atestado ou declaração de capacidade técnica, em nome da licitante, em documento timbrado, emitido por entidade da Administração Federal, Estadual ou Municipal, direta ou indireta e/ou empresa privada, que comprove que a empresa licitante tenha executado ou esteja executando serviços de características técnicas semelhantes ao objeto desta aquisição, nos termos da Lei;

3.7.2 Os atestados deverão ser acompanhados dos respectivos contratos;

3.7.3 No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa proponente. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente;

3.7.4 A comprovação deverá englobar, pelo menos, os seguintes serviços:

- Fornecimento de solução de segurança da informação, composta de pelo menos um *cluster* de equipamento do tipo *NGFW*;
- Prestação de serviço de suporte técnico para a solução de segurança;
- Disponibilização de licenças e de atualização de assinatura;
- Garantia.

3.8 Vigência

3.8.1 O contrato terá vigência de 120 (cento e vinte) dias a partir do recebimento definitivo.

3.9 Fiscalização

3.9.1 Os produtos e serviços objetos desta contratação serão fiscalizados por servidor ou comissão de servidores do Contratante, doravante denominados Fiscalização, que terá autoridade para exercer toda e qualquer ação de orientação geral, controle e fiscalização da execução contratual.

3.9.2 À Fiscalização compete, entre outras atribuições:

3.9.2.1 Solicitar à Contratada e seus prepostos, ou obter da Administração, tempestivamente, todas as providências necessárias ao bom andamento do contrato e anexar aos autos do processo correspondente cópia dos documentos escritos que comprovem essas solicitações de providências.

3.9.2.2 Manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica.

3.9.2.3 Acompanhar e atestar a prestação dos serviços contratados e indicar a ocorrência de inconformidade desses serviços ou não cumprimento do contrato.

3.9.2.4 Encaminhar à Secretaria de Administração os documentos para exame e deliberação sobre a possível aplicação de sanções administrativas.

3.9.3 A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

3.10 Recebimento do objeto

3.10.1 Para os itens 1 (*Cluster Firewall*), 2 (Software de gerenciamento) e 3 (Instalação e configuração), e em conformidade com os artigos 73 a 76 da Lei n.º 8.666/93, será aceito:

3.10.1.1 Provisoriamente, mediante recibo, imediatamente depois de efetuada a entrega do objeto, para efeito de posterior verificação de sua conformidade;

3.10.1.2 Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias úteis.

3.10.2 Para o item 4 (Treinamento), e em conformidade com os artigos 73 a 76 da Lei n.º 8.666/93, será aceito:

3.10.2.1 Provisoriamente, mediante recibo, imediatamente depois de efetuada a entrega do objeto, mediante a entrega também de lista de frequência dos participantes, para efeito de posterior verificação de sua conformidade;

3.10.2.2 Definitivamente, mediante Termo de Recebimento Definitivo, em até 10 (dez) dias úteis.

3.10.3 O objeto (item 1) deverá ser acondicionado em embalagem original lacrada, com a identificação do produto, fazendo constar sua descrição e incluindo o nome do fabricante, a marca ou modelo do material de acordo com suas características.

3.10.4 Por ocasião da entrega do objeto será requerido o fornecimento da documentação de suporte técnico e manutenção em garantia, contendo as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente, etc.).

3.10.5 Após o recebimento provisório, a fiscalização avaliará as características do objeto, identificando eventuais problemas. Estando em conformidade, será efetuado o Recebimento Definitivo.

3.10.6 Se, após o aceite provisório, constatar-se que o objeto foi entregue em

desacordo com o contrato ou com a proposta, com incorreção, ou incompleto, serão interrompidos os prazos de recebimento e suspenso o pagamento, após a notificação por escrito à Contratada e até que seja sanada a situação.

3.10.7 Os objetos entregues em desacordo com o especificado neste Termo de Referência, no Instrumento Convocatório, no Contrato ou com defeito serão rejeitados parcial ou totalmente, conforme o caso, e a Contratada será obrigada a substituí-los dentro do prazo contratual, sob pena de se considerar atraso na entrega.

3.10.8 A Contratada ficará obrigada a trocar, a suas expensas, o material que vier a ser recusado.

3.10.9 A Contratada deverá retirar o material recusado no momento da entrega do material correto. O Tribunal Superior do Trabalho não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo.

3.10.10 Será considerado abandonado o material que não for recolhido pela Contratada em até 30 dias após a comunicação da equipe do TST à Contratada.

3.10.11 A Administração poderá dar a destinação que julgar conveniente ao material abandonado em suas dependências.

3.10.12 A Contratada deverá entregar todo o material discriminado na nota de empenho, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento da obrigação.

3.10.13 Independentemente da aceitação, a Contratada garantirá a qualidade de cada unidade do produto fornecido pelo prazo estabelecido nas especificações, obrigando-se a reparar aquela que apresentar defeito no prazo estabelecido pelo Contratante.

3.10.14 O aceite provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança do serviço, nem a ético-profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela lei ou pelo contrato.

3.11 Pagamento

3.11.1 O pagamento será efetuado, em moeda corrente nacional, mediante depósito na conta bancária indicada pela Contratada, em até 10 (dez) dias úteis após o recebimento definitivo do objeto e condicionado à apresentação das notas fiscais/faturas, devidamente, atestadas pela fiscalização.

3.11.2 As notas fiscais e os documentos exigidos no edital e no contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Coordenadoria de Material e Logística, situada no SAFS, Quadra 8, Conjunto A, Bloco A, Subsolo, Brasília-DF. E-mail para contato é o cmlog@tst.jus.br.

3.11.3 Serão retidos na fonte os tributos elencados nas disposições determinadas pelos órgãos fiscais e fazendários, em conformidade com as instruções normativas vigentes.

3.12 Sanções

3.12.1 Fundamentado no artigo 49 do Decreto n.º 10.024/2019 ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até

5 (cinco) anos, garantido o direito à ampla defesa, sem prejuízo das multas previstas neste edital e das demais cominações legais, aquele que:

3.12.1.1 Não assinar o contrato;

3.12.1.2 Deixar de entregar documentação exigida neste edital;

3.12.1.3 Apresentar documentação falsa;

3.12.1.4 Ensejar o retardamento da execução do objeto;

3.12.1.5 Não mantiver a proposta;

3.12.1.6 Falhar ou fraudar na execução contratual;

3.12.1.7 Comportar-se de modo inidôneo;

3.12.1.8 Fizer declaração falsa;

3.12.1.9 Cometer fraude fiscal.

3.12.2 No caso de atraso injustificado ou inexecução total ou parcial do compromisso assumido com o TST, as sanções administrativas aplicadas à Contratada serão:

3.12.2.1 Advertência;

3.12.2.2 Multa;

3.12.2.3 Suspensão temporária de participar de licitações e impedimento de contratar com o Tribunal Superior do Trabalho;

3.12.2.4 Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

3.12.3 Durante a execução do contrato, caso existam ocorrências que ultrapassem os níveis de tolerância informados nos requisitos de prazo do objeto (vide anexo I), serão aplicadas multas, detalhadas a seguir:

- 1% (um por cento) ao dia sobre o valor referente ao respectivo item, no caso de atraso injustificado para a entrega dos equipamentos e do *software* de gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;
- 1% (um por cento) ao dia sobre o valor referente aos itens a serem instalados, no caso de atraso injustificado para conclusão do Serviço de Instalação dos Equipamentos e do *Software* de Gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;
- Para o item 1, 2% (dois por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 1 (CRÍTICA);
- Para o item 1, 1% (um por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para

o atendimento e/ou solução dos chamados abertos com nível de Prioridade 2 (ALTA);

- Para o item 1, 0,5% (meio por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (MÉDIA);
- Para o item 1, 0,25% (vinte e cinco décimos percentuais) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (BAIXA);

3.12.4 A não apresentação da comprovação de origem e quitação dos tributos de importação previstos no item 3.2.11 deste Termo de Referência implicará em multa, conforme valores estimados na tabela abaixo, bem como a sua rescisão, sem prejuízo das demais sanções previstas no art. 87 da lei 8.666/93.

Valores Contratuais		**Percentuais das multas**	**Valores Estimados da multa**	
De	**a**		**Mínimo de**	**a**
R$ 0,00	R$ 3.000,00	0,1	R$ 0,00	R$ 300,00
R$ 3.001,00	R$ 15.000,00	0,08	R$ 300,01	R$ 1.200,00
R$ 15.001,00	R$ 50.000,00	0,06	R$ 1.200,01	R$ 2.500,00
R$ 50.001,00	R$ 200.000,00	0,04	R$ 2.500,01	R$ 8.000,00
R$ 200.001,00	R$ 1.000.000,00	0,02	R$ 8.000,01	R$ 20.000,00
R$ 1.000.001,00	xxxxxxxxxxx	0,01	R$ 20.000,01	xxxx

3.12.5 A Contratada deverá justificar fundamentada, prévia e formalmente qualquer ocorrência que a leve a descumprir os deveres estabelecidos neste Termo. A aceitação da justificativa ficará a critério do Contratante.

3.12.6 As multas porventura aplicadas serão descontadas da garantia ofertada ou cobradas diretamente da Contratada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

3.12.7 As penalidades serão obrigatoriamente registradas no SICAF e sua aplicação será precedida da concessão da oportunidade de ampla defesa para o adjudicatário, na forma da lei.

3.12.8 Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei 8.666/93, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

3.12.9 Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, Quadra 08, Conjunto A, Bloco A, térreo, sala T-18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4165, (061) 3043-7570 e-mail: sgcon@tst.jus.br.

3.12.10 Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

3.13 Demais disposições

3.13.1 É de responsabilidade da Contratada o conhecimento das características do material relacionado no objeto desta licitação.

3.13.2 O TST não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros, sejam fabricantes, representantes ou quaisquer outros.

Brasília, 18 de agosto de 2020.

Integrante Demandante	Integrante Técnico	Integrante Administrativo
_____ *Leonardo Lobo Pulcineli* **Matrícula:** *42780*	_____ *Adriano Bontempo Da Silva Martinho* **Matrícula:** *39337*	_____ *Daniela Santos Teixeira* **Matrícula:** *31268*

Equipe de Planejamento e Apoio a Contratação

Anexo I

Especificação Técnica do Objeto

Requisitos Tecnológicos (hardware e software)	
ID	**Descrição**
R.HS1	Para efeitos deste Estudo Técnico, o uso das conjunções "e/ou" deve ser compreendido de forma ampla, ou seja, deve ser considerada a possibilidade de os elementos serem tomados em conjunto e, também, separadamente. Por exemplo, a expressão "Controle de políticas por porta e/ou protocolo" deve ser compreendida da seguinte forma: "O parâmetro para aplicação de políticas deve ser aplicado: a) por porta individualmente; b) por protocolo individualmente; e c) por porta e protocolo simultaneamente";
R.HS2	Cada solução de alta disponibilidade deverá ser composta por 2 (dois) equipamentos (*appliances*) funcionando em *cluster*, construídos especificamente para exercer a função de *Next Generation Firewall*, com *hardware* e *software* fornecidos pelo mesmo fabricante.
R.HS3	Deverá ser fornecida com licença(s) do(s) *software*(*s*) embutido(s) em todos os seus componentes, ou seja, durante a vigência da garantia, todas as atualizações deverão ser disponibilizadas ao Contratante. Após o seu término, a Contratante poderá continuar a utilizar o *firewall* e a console de gerência, sem as funcionalidades de NGFW;
R.HS4	Deverá ser licenciado e habilitado para uso ilimitado de usuários e endereços IP;
R.HS5	Deverá possuir ao menos as seguintes funcionalidades nativas, que deverão operar na mesma solução: • *Firewall*; • Controle de Aplicação; • Gerenciamento de Qualidade de Serviço (QoS); • Prevenção contra Ameaças (IPS, *BotNets*); • Proteção contra Ameaças Avançadas; • Identificação de Usuários; • Filtro de URL; • Rede VPN; • Console de Gerenciamento e Monitoramento;
R.HS6	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
R.HS7	Será aceita somente solução com as funcionalidades nativas descritas no item R.HS5 instaladas em ambiente físico local (*on-premise*), sendo vedada qualquer transmissão de informação para processamento na nuvem, exceto para atualização da base de dados da solução e prevenção contra ameaças avançadas;
R.HS7.1	Com relação à Proteção contra Ameaças Avançadas, poderá ser entregue equipamento físico exclusivo para essa finalidade com processamento local dos arquivos ou, caso a solução seja baseada em tratamento de dados na nuvem, essa deverá ser capaz de processar os arquivos definidos pela Contratante, independente do volume mensal, e agregar a proteção do tipo "*zero day*" par quaisquer situações;

R.HS8	Deve executar funcionalidades de proteção de rede, proteção e prevenção contra ameaças avançadas e não conhecidas, e somente será aceita solução (*hardware* e *software*) de um mesmo fabricante;
R.HS9	O *software* deverá ser fornecido em sua versão mais atualizada, relativo à data de sua instalação e configuração, não sendo permitido qualquer tipo de comprovação futura;
R.HS10	O *hardware* deve ser baseado em arquitetura que garanta flexibilidade e adaptação a novas ameaças sem impacto no desempenho;
R.HS11	A comunicação entre a solução de gerência e a solução de *hardware* de segurança, deverá ser criptografada;
R.HS12	Deve ser possível suportar arquitetura de armazenamento de *logs* redundante, permitindo a configuração de equipamentos distintos;
R.HS13	Possuir mecanismo de indexação de *logs* para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de *logs* mais antigos;
R.HS14	Os *gateways* de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;
R.HS15	Oferecer a funcionalidade de *backup*, assim como permitir ao administrador agendar procedimentos de *backups* periódicos;
	HARDWARE
R.HS16	Armazenamento de no mínimo de 1TB com 2 (dois) discos em RAID1, por equipamento, pois a falha do disco, se único, ocasionará indisponibilidade da solução bem como os dados de *log* nele existentes; • Caso a solução ofertada possua recurso de replicação síncrona de todos os dados para a solução de gerência, está será aceita.
R.HS17	Memória suficiente ou outra arquitetura que garanta desempenho sempre inferior a 75% de utilização da solução durante toda a vigência contratual; • O monitoramento poderá ser realizado tanto pelo sistema de gerenciamento centralizado ou por ferramenta própria de monitoração do TST, com intervalos mínimos de 5 minutos entre cada aferição.
R.HS18	Todos os equipamentos e seus componentes deverão ser novos, sem uso, entregues em perfeito funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.
R.HS19	Não serão aceitos equipamentos em modo *End of Life*, *End of Sale* e *End of Support*.
R.HS20	Mínimo de 4 (quatro) interfaces do tipo 10/100/1000 base-T RJ45 ou superior, com os respectivos *tranceivers*, para cada equipamento do *cluster*;
R.HS21	Mínimo de 4 (quatro) interfaces de rede do tipo 10Gbps SFP+, com os respectivos *tranceivers* bidirecional, com conector LC, para cada equipamento do *cluster*;
R.HS22	Mínimo de 4 (quatro) interfaces tipo 40Gbps QSFP+ bidirecional, com os respectivos *tranceivers* com conector LC, para cada equipamento do *cluster*;

R.HS23	Mínimo de 1 (uma) interface, dedicada para gerenciamento;
R.HS24	Mínimo de 1 (uma) interface, dedicada para console;
R.HS25	Mínimo de 1 (uma) interface, dedicada para sincronismo do *cluster*;
R.HS26	Mínimo de 1 (uma) interface, dedicada para gerenciamento *out-of-band*;
R.HS27	Fonte de alimentação 120/240 VAC, redundante e *hot-swappable*;
R.HS28	Ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0°C a 40°C.
R.HS29	Vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos, etc.) para fixação em bastidor (*rack*) padrão EIA-310 com largura de 19’’(dezenove polegadas).
R.HS30	Possuir certificação de conformidade sustentável de acordo com os padrões EPA (*Enviromental Protection Agency*) ou similar, tais como, *EnergyStar*, *RoHS* (*Restriction on Harzadous Substances*), WEEE (*Waste Electrical and Eletronic Equipament*) ou EMI *Certifications* FCC *part* 15, CE, EN55022, EN55024.
R.HS31	Possuir *throughput* de proteção de, no mínimo, 15 (quinze) Gbps para as funcionalidades de *firewall*, Controle de Aplicação, Prevenção de Ameaças (IPS, *BotNets* e Antivírus), Proteção contra Ameaças Avançadas, Filtro de URL, Identificação de Usuários da Solução, Características de *QoS*, características de VPN habilitadas simultaneamente;
R.HS31.1	O *throughput* é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Caso a fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado.
R.HS32	Suportar, no mínimo, 8.000.000 (oito milhões) de conexões concorrentes;
R.HS33	Suportar, no mínimo, 200.000 (duzentos mil) novas conexões por segundo;
R.HS34	As taxas de transferência indicadas devem ser alcançadas com a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, sem prejuízo no desempenho do equipamento, e com todas as assinaturas, lista e demais métodos de controle de acesso e de detecção e prevenção de ameaças habilitados;

	FIREWALL
R.HS35	Suportar os protocolos IPv4 e IPv6;
R.HS36	Suportar no mínimo 1024 VLANs no padrão 802.1q e estabelecer regras de filtragem (*Stateful Firewall*) entre elas;
R.HS37	Suportar agregação de *links* no padrão 802.3ad;
R.HS38	Suportar *policy based routing* ou *policy based forwarding*, possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;
R.HS39	Suportar roteamento *multicast* (PIM-SM);
R.HS40	Suportar DHCP *Relay* e DHCP *Server*;
R.HS41	Suportar *jumbo frames*;
R.HS42	Suportar NAT dinâmico (N-to-1 e N-to-N);
R.HS43	Suportar NAT estático (N-to-1 e N-to-N);
R.HS44	Suportar NAT estático bidirecional (1-to-1);
R.HS45	Suportar tradução de porta (PAT);
R.HS46	Suportar NAT de origem e NAT de destino, simultaneamente;
R.HS47	Enviar *log* para sistemas de monitoramento externos, simultaneamente aos registros internos;
R.HS48	Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (*anti-spoofing*) para IPv4;
R.HS49	Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
R.HS50	Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
R.HS51	Suportar OSPF *graceful restart*;
R.HS52	Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente e em *layer* 3;
R.HS53	Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: • Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 e camada 3; • Modo *sniffer*, para inspeção via porta espelhada do tráfego de dados da rede; • Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; • Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como *default gateway* das redes protegidas; • Modo Misto de trabalho *sniffer*, L2 e L3, em diferentes interfaces físicas.

R.HS54	A configuração em alta disponibilidade deverá ser implantada de forma a suportar *clusters* ativo/ativo e ativo/*standby*, devendo sincronizar: • Sessões; • Configurações, incluindo, mas não limitado a políticas de *firewall*; • NAT e objetos de rede; • Associação de Segurança das VPNs; • Tabelas FIB; • Tabelas de usuários autenticados.
R.HS55	O HA deve possibilitar monitoramento de falha de *link*;
R.HS56	Suportar atuação como cliente NTP (*network time protocol*);
	CONTROLE POR POLÍTICAS DE SEGURANÇA
R.HS57	A solução de segurança deve usar *Stateful Inspection* baseada na análise de comunicação e de estado da conexão para monitorar e controlar o fluxo de rede;
R.HS58	Permitir a implementação de monitoramento do segmento de Internet, através de teste de conectividade com endereços específicos, e implantar alertas em caso de quedas; • Os alertas poderão ser implementados via API.
R.HS59	As regras deverão ser elaboradas utilizando objetos de rede baseados em TCP/IP. Durante a criação da regra, tais objetos deverão ser associados sem que haja necessidade de associação à interface de rede de origem ou destino da conexão ou então permitir a configuração para todas as interfaces simultaneamente;
R.HS60	Possibilitar a configuração, entre os nós do *cluster*, no mínimo, nos modos Ativo/Ativo e Ativo/*Standby*, garantindo assim, que apenas um dos nós consiga suportar toda a demanda dessa especificação técnica;
R.HS61	Após uma queda ou reconexão de qualquer dos *links*, deve ser possível configurar ações como alertas SNMP, armazenamento do *log scripts* customizados pelo usuário;
R.HS62	Autenticar sessões ou usuários para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;
R.HS63	Controles de políticas por porta e/ou protocolo;
R.HS64	Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
R.HS65	A base de categorias e aplicações deve ser fornecida e constantemente atualizada pelo fabricante da solução, sempre que uma alteração em sua base seja feita. Deve permitir, ainda, que algum objeto seja sobrescrito por configuração do próprio administrador;
R.HS66	Controle de políticas por usuários, grupos de usuários, IPs, redes e/ou grupos de redes;
R.HS67	Controle de políticas por código de Países, sem que seja necessário configurar manualmente o escopo de endereço desses países;
R.HS68	Suportar a criação de políticas por geolocalização, permitindo que o tráfego de entrada e/ou de saída de determinado(s) país(es) seja(m) bloqueado(s);

R.HS69	Deve decriptografar tráfego *inbound* e *outbound* em conexões negociadas com, no mínimo, TLS 1.1 e TLS 1.2;
R.HS70	Bloqueio dos seguintes tipos de arquivos como *bat, cab, dll, exe, pif* e *reg* e outros, de acordo com a necessidade, configuráveis através do *software* de gerência disponibilizado;
R.HS71	*Traffic shapping* e *QoS* – priorização de tráfego de dados baseada em Políticas (Prioridade, Garantia e Limitação máxima);
R.HS72	Suporte a configuração de regras que permitam informar endereço IP nas versões IPv4 e IPv6, sem duplicação de regra;
R.HS73	Suporte a objetos e regras *multicast*;
R.HS74	Permitir o agendamento de aplicação automática de políticas em horário pré-definidos pelos administradores;
R.HS75	Deve suportar importação de certificado em inspeção de conexões SSL de entrada (*inbound*);
R.HS76	A solução deve ser capaz de identificar o comportamento do protocolo SSH, onde pode ser feito através de padrões de análise de protocolo;
R.HS77	Deve ter a capacidade de inspecionar e bloquear tráfego operando em camada 2 e camada 3;
R.HS78	Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações;
R.HS79	Deve inspecionar e bloquear os dados operando como *default gateway* das redes protegidas e controlar o tráfego em nível de aplicações;
R.HS80	Na ocorrência de falhas, as conexões existentes em um *firewall* deverão ser mantidas pelo(s) outro(s), sem perdas destas conexões, não acarretando interrupções no tráfego da rede e nem redução de desempenho da solução;
R.HS81	Na aplicação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas;
R.HS82	Promover a integração com diretório LDAP (X.500) e *Active Directory* para a autenticação de usuários, de modo que o *Firewall* possa utilizar das informações armazenadas para realizar autenticações;
R.HS83	Para configuração a administração do *Firewall* deve possibilitar o acesso via CLI (SSH), console do fabricante e interface *web* HTTPS;
R.HS84	A solução de *Firewall* deve prover funcionalidade que permita visualização do grau de utilização de cada regra, por exemplo, quantidade de *hits* por regra, % de utilização ou volume em *bytes*;
R.HS85	A solução deve, por padrão, não permitir que ataque do tipo "*scan ports*" ou similares retornem resultados do estado das portas;
R.HS86	A solução de *Firewall* deve suportar no mínimo, 10.000 (dez mil) regras;
R.HS87	A solução deve suportar o mínimo de 16.384 entradas de endereço ARP;
R.HS88	Deverá permitir a aceleração e otimização da leitura das regras, de modo que o *firewall* consiga identificar padrões muito utilizados;
R.HS89	Deverá suportar métodos de autenticação de, no mínimo, usuário e cliente;
R.HS90	A solução deverá disponibilizar interface para gerenciamento das atualizações de segurança para instalação agendada ou automática, conforme determinação da Contratante;

	CONTROLE DE APLICAÇÕES
R.HS91	A solução deverá contar com ferramentas de visibilidade e controle de aplicações *web* integradas na própria solução de segurança, que permitam a criação de políticas de liberação ou bloqueio baseando-se em aplicações *web* 2.0;
R.HS92	Deve prover o controle e a proteção de acesso à Internet por meio do reconhecimento das aplicações *web 2.0*, independente de porta e protocolo, e da classificação de URL's;
R.HS93	Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
R.HS94	Deve ser capaz de identificar um mínimo de 2.000 (duas mil) aplicações, incluindo, mas não se limitando a: *peer-to-peer*, *streaming* de áudio e vídeo, *update* de *software*, *instant messaging*, redes sociais, *proxies*, *anonymizers*, acesso e controle remoto, VoIP e e-mail;
R.HS95	Deve ser capaz de identificar, no mínimo, as seguintes aplicações: *BitTorrent*, *Youtube*, *Livestream*, *Skype*, *Viber*, *WhatsApp*, *Snapchat*, *Facebook*, *Facebook Messenger* ou *Facebook Chat*, *G Suite*, *Tinder*, *Instagram*, *Twitter*, *Linkedin*, *Dropbox*, *One* Drive ou *Microsoft One Drive*, *Logmein*, *TeamViewer*, MS-RDP, VNC, *Ultrasurf*, TOR, *Webex*, *Evernot*, *Amazon Cloud Drive*, *Gotomeeting*.
R.HS96	Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, *social widgets* (ou similar) com controle granular para usuários ou grupos de usuários;
R.HS97	A solução deverá possuir pelo menos as categorias de aplicações *web* pré-definidas pelo fabricante, atualizadas em tempo real;
R.HS98	Deve possibilitar a inspeção de tráfego HTTPS (*inbound/outbound*);
R.HS99	Deve ser capaz de identificar aplicações criptografadas usando SSL;
R.HS100	Deve possibilitar o bloqueio das aplicações, de portas e protocolos;
R.HS101	Deve possibilitar a criação de regras com várias categorias;
R.HS102	Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reiniciar os *gateways* e gerência;
R.HS103	Deve possibilitar a permissão ou bloqueio de aplicações por, pelo menos, os seguintes critérios: • Aplicação da *web*; • Categorias; • IP/Range de IP's/Redes; • Usuários do AD/LDAP; • Grupos de usuários do AD/LDAP; • Aplicações tais como *Ultrasurf*, *Torrent*, *Dropbox* e demais *File Sharing*.
R.HS104	Deve possibilitar a customização da tela de interação com o usuário, permitindo: • Informar sobre o bloqueio; • Questionar sobre a necessidade de acesso. •

R.HS105	Deve possibilitar a customização de regra utilizando as seguintes ações de controle: • Permitir; • Bloquear; • Bloquear e informar; • Monitorar; • Informar o usuário.
R.HS106	Deve permitir o bloqueio total de aplicações do tipo *proxy* (*Ultrasurf, Tor, etc.*);
R.HS107	Deve possibilitar a integração da solução com base do *Microsoft Active Directory*, LDAP, RADIUS ou base local para criação de políticas utilizando: • Usuários; • Grupo de Usuários; • Objetos cadastrados vinculados ao endereço IP; • Endereço IP; • Endereço de Rede; • Combinação das opções acima.
R.HS108	A solução deve suportar a criação de pelo menos 600 regras de controle de aplicações no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso;
R.HS109	O mecanismo de Controle de aplicação *Web*/URL deve apresentar contagem de utilização de regra de acordo com a utilização;
R.HS110	A solução deve ter um mecanismo configurável de *by-pass*, onde o administrador consegue definir grupos específicos de usuários ou de máquinas que estão autorizados a ignorar as regras de inspeção SSL;
R.HS111	Deverá categorizar as aplicações ou URL's por fator de risco;
R.HS112	A solução deverá receber atualizações, para sua base de aplicações e URL's, a partir de um serviço baseado em nuvem, fornecido pelo fabricante da solução;
R.HS113	A solução deverá possuir uma console gráfica centralizada para gerenciar regras de *firewall*, de aplicações e de URL's;
R.HS114	Deverá permitir a criação de exceções baseadas em objetos de rede;
R.HS115	A solução deve prover a opção de editar a notificação de bloqueio e redirecionar o usuário para a página de remediação;
R.HS116	Deve incluir o mecanismo de *black list* e *white list* permitindo ao administrador do sistema negar ou permitir o acesso a determinadas URL's, independente da categoria;
R.HS117	Deve inspecionar o *payload* do pacote de dados com o objetivo de detectar, através de expressões regulares (ou similar), assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não se limitando ao uso de protocolo *Remote Desktop Protocol* na porta 80 ao invés da porta 3389;

R.HS118	Para tráfego criptografado (SSL), deve decriptografar pacotes a fim de possibilitar a leitura do *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;
R.HS119	Deve realizar a decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
R.HS120	A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não se limitando a compartilhamento de arquivo de soluções;
R.HS121	Deve detectar arquivos e outros conteúdos que devem ser inspecionados de acordo com as regras de segurança implementadas em outras camadas;
R.HS122	Identificar o uso de técnicas evasivas através de comunicações criptografadas;
R.HS123	Limitar a banda (*download/upload*) usada por aplicações baseado no IP de origem, usuários e grupos do LDAP/AD;
R.HS124	Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário d rede em tempo real com integração ao *Microsoft Active Directory*, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários;
R.HS125	Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
R.HS126	Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do TST;
R.HS127	O fabricante deve permitir a solicitação de inclusão ou alteração de categorização na base de assinaturas das aplicações;
R.HS128	Deve alertar o usuário quando uma aplicação for bloqueada;
R.HS129	Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
R.HS130	Deve possibilitar a diferenciação de tráfego de *Instant Messaging* possuindo granularidade de controle e/ou políticas;
R.HS131	Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o *Whatsapp* e bloquear a transferência de arquivos;
R.HS132	Deve permitir a criação de regras de liberação e bloqueio utilizando apenas o domínio, usando expressões regulares, sem necessidade de inserção do endereço IP pelo administrador, onde a resolução deve ser feita de forma automática e em tempo real pela solução, inclusive para consultas baseadas em nuvem.
R.HS133	Deve ser possível a criação de grupos estáticos e dinâmicos de aplicações;
	PREVENÇÃO DE AMEAÇAS
R.HS134	Deve incluir assinaturas de prevenção de intrusão, IPS, e suporte ao bloqueio de arquivos e códigos maliciosos;

R.HS135	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar: *Antivírus*, *Antimalware* e *BotNets* integrados na própria solução de *firewall* sem a necessidade de uso de quaisquer interfaces externas, onde sua console de gerência deverá residir na mesma console centralizada;
R.HS136	Deve sincronizar as assinaturas de prevenção de ameaças por demanda ou por agendamento;
R.HS137	As assinaturas devem permitir a ativação e desativação, ou ainda, ativação apenas em modo de monitoramento;
R.HS138	Exceções por IP de origem ou destino devem ser possíveis, de forma geral e assinatura-a-assinatura;
R.HS139	Deve suportar granularidade nas políticas de *Antivírus* e *Antimalware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, grupo de usuários, serviço ou assinatura e a combinação de todos esses itens;
R.HS140	Deve suportar o bloqueio de vulnerabilidades;
R.HS141	Deve incluir proteção contra ataque de negação de serviços (*DoS* e *DDoS*);
R.HS142	Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos os seguintes ataques conhecidos: SQL *Injection*, ICMP *denial of servisse*, força bruta e *port scanner*, SMB, *Port overflow*, *Non compliant* SSL;
R.HS143	Deverá possuir mecanismos de detecção de assinaturas, anomalias de protocolos, controle de aplicações e detecção de comportamento;
R.HS144	A solução de IPS deve fazer a inspeção de toda a sessão, independentemente do tamanho, de forma bidirecional, sem degradas o desempenho do equipamento;
R.HS145	O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar a solução;
R.HS146	Deve estar incluso informações como código CVE (*Common Vulnerabilities and Exposures*), severidade e tipo de ação a ser executada em cada proteção de segurança, mesmo que de forma manual;
R.HS147	Deve ser capaz de bloquear tráfego SSH enviado em portas diferentes da porta padrão;
R.HS148	As regras de exceção deverão possuir origem, destino, serviço, severidade, grupo de usuário ou alguma dessas combinações;
R.HS149	A solução deve ser capaz de inspecionar tráfego HTTPS de entrada e saída;
R.HS150	A solução de IPS integrada na solução de segurança deve possuir uma base de assinatura não inferior a 10.000 (dez mil) assinaturas;
R.HS151	A solução de IPS deve possuir funcionalidade que permita configurar as assinaturas do IPS o modo apenas de detecção para fins de *troubleshooting*;
R.HS152	A solução de IPS deve possuir índices por período que apontem o nível de ação das assinaturas baseado pela sua severidade na própria interface de gerência;

R.HS153	A solução deve permitir incorporar de forma automática novas proteções de IPS através de sua severidade;
R.HS154	O módulo de IPS deve possuir assinaturas voltadas para ambiente de servidores *web* e DNS;
R.HS155	A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação protegendo, pelo menos, os seguintes serviços: Aplicações *web*, serviços de e-mail, DNS, FTP, serviços *Windows* (*Microsoft Networking*) e VoIP;
R.HS156	A solução deve permitir ao administrador configurar quais métodos e comandos HTTP e comandos FTP são permitidos e quais são bloqueados;
R.HS157	Deve incluir proteção contra vírus e *worms* em conteúdo *ActiveX*, *applets Java* e outros;
R.HS158	Deve possuir perfis pré-configurados de proteção de IPS que podem ser utilizados a qualquer momento;
R.HS159	Deve incluir tela de visualização a fim de monitorar graficamente a quantidade de alertas de diferentes severidades. As diferentes áreas de interesse devem ser definidas utilizando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades da solução, incluindo pelo menos: origem, destino, serviço, usuário, tipo e nome do alerta;
R.HS160	A solução deve permitir a configuração de inspeção do IPS baseada em políticas que utilizem o posicionamento geográfico de origens ou destinos e combinações entre os dois;
R.HS161	A solução de possuir esquemas de atualização de assinaturas, no mínimo, através de agendamento, modo *off-line* e por demanda;
R.HS162	A solução deverá possuir relatório e correlação de eventos centralizada;
R.HS163	A solução deverá permitir a ativação de novas proteções baseada em parâmetros configuráveis como: severidade da ameaça, proteções para clientes e proteções para servidores;
R.HS164	A solução deve proteger contra ataques do tipo DNS *Cache Poisoning* e impedir que os usuários acessem endereços de domínios bloqueados;
R.HS165	A solução deve permitir bloquear o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente o *range* de endereços IP dos países que se deseja bloquear;
R.HS166	Ser imune e capaz de impedir ataques básicos como: SYN *flood*, ICMP *flood*, UDP *flood*;
R.HS167	Suportar análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
R.HS168	A solução deverá realizar análise de *malware*, em sistemas físicos exclusivos (*bare metal*), evitando a atuação de *malwares* que reconheçam sistemas de *sandbox*;
R.HS169	Deverá ser capaz de decriptografar para análise pelo menos o protocolo SSL;
R.HS170	Deverá ser capaz de implementar autenticação para aplicações de multifator (MFA) ;
R.HS171	Detectar e bloquear a origem de *port scans*;

R.HS172	Possuir assinaturas para bloqueio de ataques de *buffer overflow*;
R.HS173	Suportar o bloqueio de vírus e *spywares*;
R.HS174	Suportar bloqueio de arquivos por tipo ou extensão;
R.HS175	Identificar e bloquear comunicação com *BotNets*;
R.HS176	Deve suportar referência cruzada com CVE (*Common Vulnerabilities and Exposures*);
R.HS177	A solução deve possuir nuvem de inteligência proprietária do fabricante, que seja responsável em atualizar toda a base de segurança do *appliances* através de assinaturas, durante a vigência do contrato;
R.HS178	Implementar modo de configuração totalmente transparente para o usuário final de modo que não haja necessidade de configuração de *proxies*, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
R.HS179	Implementar funcionalidade de detecção e bloqueio de *call-backs* (comunicação do *malware* com o servidor de comando e controle);
R.HS180	A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede, baseado em análises de tráfego de rede, processamento de pacotes, dentre outros;
R.HS181	A solução de proteção contra *BotNets* deve utilizar mecanismo de detecção em multicamadas, que inclui reputação ode endereço IP, URLs e endereços DNS, assim como detecção de padrões de comunicação BOT;
R.HS182	O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regras individuais visando aperfeiçoar o desempenho do equipamento;
R.HS183	A solução de segurança deve permitir o bloqueio de *download* de arquivos que exceda tamanho pré-definido;
R.HS184	A solução deve analisar e bloquear *malwares* e/ou códigos maliciosos pelo menos nos seguintes tipos de arquivos do pacote *office* (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), MacOS (*mach*-O, DMG e PKG), *Linux* (ELF), RAR e 7-ZIP, análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL;
R.HS185	A solução deve realizar a análise dos arquivos de *download* anteriormente a entrega ao usuário;
R.HS186	Possuir antivírus em tempo real para ambiente de *gateway* internet, integrado à plataforma de proteção para os protocolos HTTP, HTTPS e SMTP;
R.HS187	A solução deve atuar na prevenção de forma granular através de políticas por usuário/máquina ou rede, sendo possível escolher um perfil diferente para cada regra ou prover todas as informações necessárias no *log* para a criação da exceção de forma manual;
R.HS188	A solução deve permitir criar regras de exceção de acordo com a proteção a partir do *log* visualizado na interface gráfica da gerência centralizada;
R.HS189	A solução de relatório deve apresentar via interface gráfica, no mínimo, informações de *hosts* infectados, atividades de *malware* e detalhes dos alertas;

R.HS190	Deve possuir visualização na própria interface de gerência dos maiores incidentes através de *hosts* ou incidentes de vírus e *bots*;
R.HS191	A solução deve permitir compartilhar informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do fabricante;
R.HS192	Permitir o bloqueio de *malwares*;
R.HS193	A solução deverá ser capaz de manter a análise de antivírus em caso de falha de conexão com a nuvem, bem como permitir criação de regras exceção para análise de antivírus;
R.HS194	A solução deverá possuir mecanismo para proteger contra ataques de *phishing*;
R.HS195	A solução deve ser capaz de proteger contra ataques DNS, tais como capacidade de detectar e prevenir C&C DNS *Hide Out*, analisar padrões de comunicação C&C e não apenas o servidor DNS de destino, realizar engenharia reversa do *malware*, detecção passiva de DNS e de comando e controle (C&C) e capacidade para detectar e prevenir ataques DNS *tunneling*;
R.HS196	A solução deverá suportar análise de arquivos que trafegam dentro do protocolo SMB, versões 2 e 3;
R.HS197	Deve suportar a inspeção em arquivos compactados;
	PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS
R.HS198	A solução deverá prover as funcionalidades de inspeção de tráfego de entrada de *malwares* não conhecidos (APT *Advanced Persistent Threat* e *Zero-Day Threats*), *ransomwares* com filtro de ameaças avançadas e análise de execução em tempo real e inspeção de tráfego de saída de *call-backs*;
R.HS199	Possuir capacidade de prevenção de ameaças não conhecidas;
R.HS200	A solução deve possuir funcionalidades para prevenção de *malwares* não conhecidos, incluídas na própria ferramenta (*zero-day*);
R.HS201	Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP;
R.HS202	Deve ser capaz de inspecionar tráfego criptografado usando SSL;
R.HS203	A solução deve possuir mecanismo para identificar *hosts* infectados tentando acessar endereços de DNS de domínios maliciosos;
R.HS204	Suportar o bloqueio automático de domínios maliciosos identificados com análise em tempo real;
R.HS205	Suportar a detecção de controle ou o roubo de dados usando tunelamento de DNS;
R.HS206	Suportar respostas dinâmicas automatizadas para encontrar máquinas infectadas;
R.HS207	Implementar e identificar existência de *malware* em anexos de e-mail e URL's conhecidas;
R.HS208	A solução deve possuir *engine* que seja possível não analisar determinada origem e/ou destino, configurados pelo administrador;
R.HS209	Identificar e bloquear a existência de *malware* em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

R.HS210	Possuir mecanismo de bloqueio de vazamento, em tempo real, não intencional de dados originados de máquinas existentes no ambiente LAN de acordo com a classificação interna do arquivo;
R.HS211	Possuir funcionalidade de detecção e bloqueio imediato de *malwares* que utilizem mecanismo de exploração em arquivos no formado PDF;
R.HS212	A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais e aplicativos;
R.HS213	A tecnologia de máquina virtual em ambiente local ou de nuvem deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do *malware* ou código malicioso sem utilização de assinaturas;
R.HS214	Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema.
R.HS215	As atualizações deverão ser fornecidas pelo fabricante;
R.HS216	A solução deve possuir nuvem de inteligência proprietária do fabricante que seja responsável por atualizar toda a base de segurança através de assinaturas;
R.HS217	Implementar mecanismo de integração com servidores *syslog*;
R.HS218	A solução deve suportar as topologias de implantação *Inline* e *Mirror/*TAP;
R.HS219	A solução deve apresentar informações comportamentais, incluindo listagem de módulos e processos utilizados por *malware* e/ou código malicioso de forma sequencial;
R.HS220	Toda a análise e bloqueio de *malwares* e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato. Não serão aceitas soluções que apenas detectam o *malware* e/ou códigos maliciosos;
R.HS221	Implantar mecanismo do tipo de múltiplas fases para verificação de *malware* e/ou códigos maliciosos;
R.HS222	Deve possuir mecanismo de exceção, permitindo criação de regras por VLAN, subrede, endereço IP, grupo de usuários, domínio de destino, entre outros;
R.HS223	Implementar através da interface gráfica mecanismo de atualização da base de dados, sistema operacional e de *firmware* da solução;
R.HS224	A solução deve emular e eliminar *malwares* conhecidos em anexos de e-mail e documentos baixados na *web*;
R.HS225	A solução deve suportar a detecção e prevenção de vírus *cryptors* & *ransomware* e seus variantes, utilizando análises estáticas e dinâmicas;
R.HS226	O sistema de análise local deve prover informações sobre as ações da ameaça na máquina infectada, informações sobre quais aplicações são usadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *malware*, gerar assinaturas de contenção automaticamente, definir URL's não confiáveis utilizadas pelo novo *malware* e prover informações sobre o usuário infectado;
R.HS227	O sistema automático de análise local ou na nuvem deve emitir relatório com identificação do *malware*;

R.HS228	O sistema de emulação deve exibir a quantidade de arquivos analisados ou permitir a visualização de todos os arquivos analisados;
R.HS229	A solução deve possuir capacidade de executar arquivos em um ambiente simulado e controlado, local ou em nuvem;
R.HS230	Permitir o envio de arquivos para análise ambiente controlado de forma automática;
R.HS231	Suportar a análise de tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
R.HS232	Caso sejam necessárias licenças de sistema operacional e *softwares* para execução de arquivos no ambiente controlado, essas deverão ser fornecidas em sua totalidade sem custos adicionais;
R.HS233	A solução deverá possuir os indicadores referentes ao último dia, última semana ou últimos 30 dias para arquivos inspecionados e arquivos maliciosos encontrados;
R.HS234	Deve permitir exportar o resultado das análises de *malwares* de *zero-day* em PDF ou CSV, a partir da própria interface de gerência;
	FILTRO DE URL
R.HS235	Para prover maior visibilidade e controle dos acessos dos usuários do ambiente a solução deve incluir módulo de filtro de URL integrado;
R.HS236	Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
R.HS237	Deve ser possível criar políticas por usuários, grupo de usuários, IP's, redes e grupos de redes;
R.HS238	Deverá possuir um mecanismo para informar ou perguntar ao usuário, em tempo real, com a finalidade de educa-los ou confirmar ações baseadas na política de acesso;
R.HS239	O mecanismo de controle de aplicação *web/url* deve apresentar contagem de utilização da regra;
R.HS240	A solução de Filtro de URL deverá ser totalmente integrada às Aplicações *Web* 2.0;
R.HS241	Deve possibilitar a inspeção de tráfego HTTPS;
R.HS242	A solução deve suportar a criação de mais de 600 regras de controle URL no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso;
R.HS243	A solução deve possuir *engine* de bloqueio de busca como *Google*, *Bing* e *Yahoo* independentemente se a opção *Safe Search* está habilitada no navegador do usuário;
R.HS244	Deverá permitir o controle, sem instalação de cliente de *software*, em equipamentos não autenticados, através de *Captive Portal*;
R.HS245	Equipamentos e usuários autenticados pelo *Active Directory* devem ser classificados de forma transparente de acordo com as políticas configuradas;
R.HS246	Deverá possuir suporte a identificação de usuários em *Microsoft Terminal Server*, permitindo visibilidade e controle sobre o uso das URL's que estão sendo acessadas através destes serviços;

R.HS247	A solução deve fornecer mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
R.HS248	Deverá incluir capacidade de configuração de políticas baseadas na visibilidade e controle de quem está usando tais URL's, através da integração com serviços de diretório, autenticação LDAP, *Active Directory* e base de dados local;
R.HS249	Suportar a criação de políticas baseadas no controle por URL e categoria de URL;
R.HS250	A solução deve ter uma base de URL que exceda 40 (quarenta) milhões de URL's categorizadas na base de dados do fabricante;
R.HS251	Suportar armazenamento de URL na própria solução evitando *delay* de comunicação/validação de URL's;
R.HS252	Suportar a criação de categorias de URL's customizadas;
R.HS253	Suportar a exclusão de URL's do bloqueio por categoria;
R.HS254	Permitir a customização da página de bloqueio que será mostrada para o usuário;
R.HS255	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário;
	IDENTIFICAÇÃO DE USUÁRIOS DA SOLUÇÃO
R.HS256	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando as aplicações e URL's através da integração com serviços de diretório, autenticação via LDAP, *Microsoft Active Directory*, RADIUS e base de dados local;
R.HS257	Deve possuir integração com *Microsoft Active Directory*, em diversos domínios simultaneamente para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupo de usuários sem a necessidade de instalar nenhum agente nos servidores *Active Directory* ou em máquina da rede;
R.HS258	Deve suportar o recebimento de eventos de autenticação de controlador wireless, dispositivo 802.1x, RADIUS ou *syslog*, para correlacionar endereços IP e usuários;
R.HS259	Para usuários não registrados ou não reconhecidos no domínio a solução deve ser capaz de fornecer uma autenticação baseada em navegador (*Captive Portal*), sem a necessidade de agente;
R.HS260	Deve possuir também suporte a autenticação via *Kerberos*;
R.HS261	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em *Microsoft Terminal Server*, permitindo visibilidade e controle granular;
R.HS262	A solução deverá ser capaz de identificar nome do usuário, *login* e IP registrados no *Microsoft Active Directory* de forma transparente para o usuário sem a necessidade de uso de agentes;
R.HS263	A solução deve suportar a opção de instalação de agentes em estações que possuam múltiplos usuários conectados simultaneamente com a finalidade de diferenciar os diferentes perfis em uso;
R.HS264	A solução deverá compartilhar e propagar a identificação de usuários com outros *gateways* de segurança do mesmo *cluster*;

R.HS265	Na integração com o *Active Directory*, todos os controladores de domínio em operação devem ser cadastrados sem a utilização de *scripts* de comando;
R.HS266	A solução de identificação de usuário deverá se integrar com as funcionalidades de *firewall*, controle de aplicação *web*, URL e Proteção contra Ameaças, sendo todas elas do mesmo fabricante e na mesma console de gerência;
	CARACTERÍSTICAS DE QOS
R.HS267	Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário;
R.HS268	Suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e *WhatsApp*);
	CARACTERÍSTICAS DE VPN
R.HS269	Deve disponibilizar licenciamento para VPN *site-to-site* e *client-to-site*, de forma a atender os itens abaixo;
R.HS270	Suportar, no mínimo, 1.000 (um mil) túneis VPN IPSec simultâneos;
R.HS271	Suportar, no mínimo, 5.000 (cinco mil) usuários VPN SSL;
R.HS272	Suportar VPN *site-to-site* em topologia *Full Meshed* (todos os *gateways* possuem *links* específicos para todos os demais *gateways*);
R.HS273	Suportar criptografia AES-128, AES-256;
R.HS274	Suportar integridade de dados com SHA-1 e SHA-256;
R.HS275	Suportar o protocolo IKE, fases I e II;
R.HS276	Suportar os algoritmos RSA e *Diffie-Hellman groups* 1, 2, 5 e 14;
R.HS277	Suportar NAT-T (NAT *Transversal*);
R.HS278	Suportar VPN IPSec *client-to-site*;
R.HS279	Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional e sem limite do número de usuários;
R.HS280	O cliente de VPN *client-to-site* deve ser compatível ou suportar o cliente nativo de pelo menos: Windows 10 (32 e 64 Bits), Apple IOS, Android, Mac OSx 10 ou Linux. Pode fornecer também, mas não obrigatória opção *Clientless* com autenticação via *browser*, para fechar a VPN através de um portal SSL;
R.HS281	Suportar atribuição de endereço IP nos clientes remotos de VPN;
R.HS282	Suportar atribuição de DNS nos clientes remotos de VPN;
R.HS283	Suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF ou BGP;
R.HS284	O túnel VPN do cliente ao *gateway* (*client-to-site*) deve fornecer uma solução de autenticação única (*sigle-sign-on*) aos usuários, integrando-se com as ferramentas de *Windows login*;
R.HS285	Deve permitir criar políticas por usuários e grupos para tráfego de VPN *client-to-site*;
R.HS286	Suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado ou CA externa de terceiros;

R.HS287	Deve promover a integração com diretórios *Active Directory* para a autenticação de usuários de VPN e regras de acesso;
R.HS288	Suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha do *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado ou CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
R.HS289	Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKLCS#12;
R.HS290	Suportar a solicitação de emissão de certificados a uma autoridade certificadora de confiança (*enrollment*) via SCEP (*Simple Certificate Enrollment Protocol*) ou CSR (*Certificate Signing Requests*);
R.HS291	Suportar a leitura e verificação de CRLs (*certification revogation lists*);
R.HS292	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

Requisitos Tecnológicos (Software de Gerência)	
ID	**Descrição**
R.SG1	A solução de gerência deverá ser separada dos *gateways* de segurança. Esta irá gerenciar as políticas de segurança de todos os *firewalls* vinculados e funcionalidades solicitadas. Deverá ainda armazenar *logs* e produzir relatórios de forma unificada;
R.SG2	A solução deve, preferencialmente, ser do tipo "*appliance virtual*" – solução de *software* baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF (*Distributed Management Task Force*), ou sistema operacional desenvolvido pelo próprio fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual – compatível com *VMWare vSphere* 6 ou superior. Será aceito combinação de dois *appliances virtuais* para compor solução de gerenciamento centralizado e armazemanento de logs;
R.SG3	Caso seja ofertada solução em *appliance* físico, a solução deve atender a todas as exigências previstas para a solução fornecida em *appliance virtual*, devendo ser fornecido com configuração de CPU e memória (RAM e *Flash*) suficiente para implementação de todas as funcionalidades descritas nesta especificação, simultaneamente;
R.SG4	Caso a solução ofertada seja em *appliance* físico a utilização de memória e CPU não deve exceder 70% de utilização;
R.SG5	Caso seja ofertada solução em *appliance* físico, esta deverá ser fornecida em alta disponibilidade, de modo que a falha de um equipamento não cause a indisponibilidade da solução de gerenciamento;
R.SG6	Deve estar licenciada e permitir a gerência centralizada de todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade;

R.SG7	Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada, no mínimo, a de capacidade de armazenamento local de *logs* indexados por no mínimo 100 dias, assim como deve suportar uma capacidade mínima de 3TB de armazenamento total de *logs* indexados;
R.SG8	Deve estar licenciada para o limite máximo de usuários objetos, regras de segurança, NAT e endereços IP suportados pela solução;
R.SG9	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contexto que compõem a solução de alta disponibilidade;
R.SG10	Deve permitir a criação de distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os *clusters*;
R.SG11	Suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de *Next Generation Firewall*, filtragem de URLs, monitoração de *logs*, *debugging*, *troubleshooting*;
R.SG12	Deve possuir a capacidade de definir administradores com diferentes perfis de acessos. Os perfis de acesso devem ser no mínimo de leitura/escrita e somente leitura;
R.SG13	Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterar configurações, ler configurações, etc.;
R.SG14	Deve permitir a delegação de funções de administração;
R.SG15	Suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente;
R.SG16	Deve registar em *log* de auditoria as ações dos usuários administradores;
R.SG17	Suportar a identificação e utilização de usuários nas políticas de segurança;
R.SG18	Suportar agrupamento lógico de objetos (*object grouping*) para criação de regras;
R.SG19	Deve incluir a opção de segmentar a base de regra utilizando rótulos ou Títulos de seção para melhor organizar a política;
R.SG20	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas;
R.SG21	Deve contabilizar a utilização (*hit counts*) ou o volume de dados trafegados correspondentes a cada regra de filtragem (*Access Control Entry*) individualmente;
R.SG22	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês ano, dia da semana e hora);
R.SG23	Deve permitir distribuição centralizada de pacotes de atualização;
R.SG24	Deve ser capaz de testar a conectividade dos equipamentos gerenciados;

R.SG25	Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;
R.SG26	Deve permitir localizar em quais regras um objeto está sendo utilizado;
R.SG27	Deve prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto de regras que possa ser condensado em uma única regra;
R.SG28	Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);
R.SG29	Suportar a geração de alertas automáticos via e-mail, SNMP ou *syslog*;
R.SG30	Suportar *rollback* de configuração para a última configuração salva;
R.SG31	Deve permitir validar as regras antes de aplica-las;
R.SG32	Deve permitir a visualização e comparação das configurações atual, anterior e antigas;
R.SG33	Deve permitir a exportação automática e agendada de *logs* via SCP;
R.SG34	Deve possuir relatórios de utilização dos recursos por, no mínimo, aplicação ou categoria, usuários, IP de origem/destino;
R.SG35	Deve possuir visualização sumarizada de todas as aplicações, ameaças e URL's que foram identificadas e controladas pela solução;
R.SG36	Deve permitir a criação de relatórios customizados;
R.SG37	Deve possibilitar a filtragem dos *logs* do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário;
R.SG38	Deve possuir relatório com informações consolidadas sobre as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços, ou mais frequentes ataques e ameaças de segurança, detectados com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários maiores consumidores de banda de Internet, os sítios na Internet mais visitados;
R.SG39	Deve ser gerado relatório caso a abertura do *link* pela *Sandbox* o identifique como site hospedeiro de *exploits* ou *malware*;
R.SG40	Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
R.SG41	A *Sandbox* deve prover informações sobre as ações do *malware* na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *malware*, gerar assinatura de antivírus e *Anti-spyware* automaticamente, definir URL's não confiáveis utilizadas pelo novo *malware* e prover informações sobre o usuário infectado;
R.SG42	Deve permitir a geração automática e agendada dos relatórios;
R.SG43	Deverá permitir seu gerenciamento por CLI (*Command Line Interface*), via SSH, *Web* GUI utilizando HTTPS ou console gráfica proprietária do fabricante;
R.SG44	Deve possuir mecanismo de ajuda de comandos via SSH, facilitando a localização e parâmetros dos mesmos;

R.SG45	Deve possuir console de *log* onde é possível visualizar os *logs* em tempo real, permitindo ao administrador realizar as devidas análises para fins de *troubleshooting*;
R.SG46	Deverá prover fácil administração na aplicação das políticas para os *gateways*, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos *gateways* remotos em uma única sessão, evitando qualquer tipo de retrabalho de configuração e reaplicação de regra;
R.SG47	Deve possuir console de visualização da topologia dos *firewalls* gerenciados, de forma centralizada;
R.SG48	Deve prover informações do status de todos os túneis VPN, incluindo: • Túneis permanentes e seu estado de conexão; • Túneis e suas comunidades; • Usuários conectados utilizando a VPN "*client-to-site*";
R.SG49	Deverá prover informações gerais de cada *gateway* como volume de pacotes aceitos, conexões concorrentes, novas conexões e licenciamento;
R.SG50	O monitoramento deverá ser capaz de monitorar todos os usuários remotos conectados;
R.SG51	Deve ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, assim como registrar e alertar quando o túnel VPN estiver desconectado;
R.SG52	Deve possuir recurso de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (*shadowing*);
R.SG53	Deve suportar a programação de relatórios automáticos;
R.SG54	Deverá permitir exportar o resultado das análises de *malwares* de dia Zero em PDF a partir da própria interface de gerência;
R.SG55	Deverá permitir o *download* dos *malwares* identificados a partir da própria interface de gerência;
R.SG56	Deverá permitir visualizar os resultados das análises de *malwares* de dia Zero nos diferentes sistemas operacionais suportados;
R.SG57	Deverá permitir informar ao fabricante quanto a suspeita de ocorrências de falso positivo e falso negativo na análise de *malwares* de dia Zero a partir da própria interface de gerência;

Requisitos de Instalação e Configuração	
ID	**Descrição**
R.IC1.	A instalação dos equipamentos deverá ser realizada no *DataCenter* do Tribunal Superior do Trabalho;
R.IC2.	Todo ferramental necessário para execução dos serviços de instalação, configuração inicial, incluindo *softwares*, equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da CONTRATADA;
R.IC3.	A CONTRATANTE disponibilizará o espeço no *DataCenter*, assim como a infraestrutura elétrica até a posição onde será instalados equipamentos;
R.IC4.	O equipamento deverá ser instalado na última versão de *firmware* disponível pelo fabricante;

R.IC5.	Entende-se por configuração inicial para efeito deste estudo: • Elaboração em conjunto com a equipe técnica do TST, de projeto de configuração, segundo as melhores práticas do fabricante e considerando as demandas e características dos serviços do CONTRATANTE; • Realização da configuração inicial do equipamento ofertado, segundo projeto, e conforme padrão de endereçamento IP a ser fornecido pelo CONTRATANTE; • Realização de migração e adequação das regras vigentes no CONTRATANTE, de forma automatizada;

Requisitos de Treinamento (Capacitação)	
ID	**Descrição**
R.T1	A Contratada deverá fornecer treinamento oficial do fabricante, podendo ocorrer nas dependências do TST ou em local próprio indicado pela Contratada;
R.T2	Todos os custos envolvidos com o treinamento deverão ser de responsabilidade da Contratada, incluindo material didático, hospedagem e passagem (dos alunos), caso não seja realizado em Brasília;
R.T3	O treinamento poderá ser oferecido na modalidade EaD;
R.T4	O treinamento deverá ser focado na aprendizagem e no desenvolvimento de habilidades práticas necessárias para configurar e gerenciar o ambiente;
R.T5	O treinamento deverá ter carga horária de, no mínimo, 40 (quarenta) horas;
R.T6	Caso haja necessidade de carga horária superior a 40 (quarenta) horas, deve haver um intervalo de, no mínimo 1 (uma) semana e no máximo 3 (três) semanas entre os módulos;
R.T7	Os cursos deverão habilitar o participante a gerenciar a solução e a realizar configurações referentes às funcionalidades especificadas nos requisitos tecnológicos.
R.T8	Os certificados deverão ser entregues no prazo de 10 (dez) dias corridos contados após o término do treinamento, sem ônus adicional para a CONTRATANTE;
R.T9	Deverá ser fornecido treinamento para 5 (cinco) servidores indicados pelo CONTRATANTE

Requisitos Legais, Sociais e Ambientais	
ID	**Descrição**
R.LSA01	A empresa deverá estar habilitada juridicamente (art. 28 da Lei n.º 8.666/93) e em regularidade fiscal e trabalhista (art. 29 da Lei n.º 8.666/93).
R.LSA02	Decreto Nº 2.271 de 7 de Julho de 1997, que dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências

R.LSA03	Resolução CNJ nº 182/2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.
R.LSA04	Decreto-lei N.º 5.452, de 1º de Maio de 1943, que define a Consolidação das Lei do Trabalho.
R.LSA05	Súmula nº 269 do TCU que estabelece que nas contratações para a prestação de serviços de Tecnologia da Informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis mínimos de serviço.
R.LSA06	Cumprir o disposto no inciso XXXIII do art. 7.º da Constituição Federal de 1988, quanto ao emprego de menores.
R.LSA07	Promover a correta destinação dos resíduos resultantes da prestação do serviço, tais como peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental como a Política Nacional de Resíduos Sólidos (Lei n.º 12.305/2010) e o Guia de Contratações Sustentáveis da Justiça do Trabalho (Resolução n.º 103/2012 do Conselho Superior da Justiça do Trabalho).
R.LSA08	Prever a destinação ambiental adequada das pilhas e baterias usadas ou inservíveis, segundo disposto na Resolução CONAMA nº 257, de 30 de junho de 1999.
R.LSA09	Os equipamentos devem obrigatoriamente estar em conformidade com o artigo 55 da Resolução 715 de 23 de outubro de 2019, emitida pela ANATEL;
R.LSA10	Possuir certificação de conformidade sustentável de acordo com os padrões EPA (*Enviromental Protection Agency*) ou similar, tais como, *EnergyStar*, *RoHS* (*Restriction on Harzadous Substances*), WEEE (*Waste Electrical and Eletronic Equipament*) ou EMI *Certifications* FCC *part* 15, CE, EN55022, EN55024.

Requisitos de Manutenção	
ID	**Descrição**
R.M1	Elaboração do plano de implementação dos novos equipamentos e *software* de gerenciamento, envolvendo: • Instalação dos equipamentos novos, sem prejuízo da operação da rede atual;
R.M2	Documentação de Planejamento e implementação detalhada da solução;
R.M3	Substituição dos *firewalls* existentes;
R.M4	Configuração das funcionalidades Next Generation *Firewall*, IPS, proteção avançada contra ameaças, QoS, controle de aplicativos e VPN IPSEC;
R.M5	Migração das políticas de segurança existentes;
R.M6	Criação dos usuários administradores;
R.M7	Criação de perfis de usuários da VPN IPSEC;
R.M8	Customização de regras de acesso de acordo com as necessidades do TST;
R.M9	Integração com o *Active Directory*;

R.M10	Realização de *backup* das configurações;
R.M11	Operação Assistida de Funcionamento da Solução, que consiste da disponibilização de um técnico residente, das 8h às 17h, com intervalo para almoço, no endereço do Contratante, devidamente identificado, para sanar quaisquer dúvidas e problemas que ocorrerem na operação da solução, durante 3 dias. Este técnico deverá ser certificado pelo fabricante do equipamento.
R.M12	Testes de Aceite e Funcionamento;
R.M13	Fornecimento da documentação de todo o projeto;
R.M14	A instalação dos equipamentos deverá ser efetuada pela Contratada ou Fabricante, conforme orientação do Serviço de Infraestrutura do Órgão da JT Contratante, observados os seguintes itens: • Todos os componentes necessários para o correto funcionamento dos equipamentos ofertados devem ser fornecidos pela Contratada;
R.M15	Caberá à Contratada ou Fabricante a montagem dos equipamentos no RACK já existente.

Requisitos de Prazo	
ID	**Descrição**
R.P1	A entrega total dos equipamentos e *software*, objeto da ordem de fornecimento deverá ocorrer em até 60 (sessenta) dias corridos e contados após a assinatura do Contrato;
R.P2	A instalação, configuração e migração das regras deverá ocorrer em até 30 dias após a entrega dos equipamentos;
R.P3	O fornecedor contratado deverá assegurar a disponibilidade da solução conforme os **Níveis Mínimos de Serviço (NMS)**, através de número telefônico específico para o fim ou e-mail na forma abaixo estabelecida:
R.P4	No momento da abertura do chamado, será informada a prioridade para o atendimento de acordo com as seguintes definições: • **Prioridade 1 (Crítica)**: Este Nível de severidade é aplicado em situações de emergência ou problema crítico, caracterizado pela existência de ambiente paralisado. • **Prioridade 2 (Alta)**: Este nível de severidade é aplicado em situações de alto impacto, incluindo os casos de degradação severa de desempenho da solução. Também se aplica a esta severidade casos onde um *appliance* para de funcionar, ocasionando a perda da alta disponibilidade da solução. Outros exemplos para esta severidade: Perda de redundância, reinicialização de módulos, slots ou portas com defeitos, perda de funcionalidades. • **Prioridade 3 (Média)**: Este nível de severidade é aplicado em situações de baixo impacto ou de problemas que se apresentam de forma intermitente. • **Prioridade 4 (Baixa)**: Este nível de severidade é aplicado em situações de dúvidas técnicas em relação ao uso ou à implementação da solução.

<table>
<tr><td>R.P5</td><td>
<table>
<tr><td rowspan="2">PRAZOS</td><td colspan="4">PRIORIDADE</td></tr>
<tr><td>1
(Crítica)</td><td>2
(Alta)</td><td>3
(Média)</td><td>4
(Baixa)</td></tr>
<tr><td>Início do atendimento</td><td>Até 30 minutos após a abertura do chamado</td><td>Até 1 hora após a abertura do chamado</td><td>Até 4 horas após a abertura do chamado</td><td>Até 8 horas após a abertura do chamado</td></tr>
<tr><td>Solução Definitiva</td><td>Em até 6h do início do atendimento</td><td>Em até 12h do início do atendimento</td><td>Em até 24h do início do atendimento</td><td>Em até 72h do início do atendimento</td></tr>
<tr><td>Tolerância mensal de descumprimentos</td><td>0</td><td>1</td><td>2</td><td>2</td></tr>
</table>
</td></tr>
<tr><td>R.P6</td><td>Em caso onde ocorram descumprimentos de NMS que se enquadre nos valores de tolerância acima informados, a empresa será notificada e advertida do não cumprimento do acordo de nível de serviço;</td></tr>
<tr><td>R.P7</td><td>Caso existam ocorrências que ultrapassem os níveis de tolerância informados na tabela acima, serão aplicadas as seguintes penalidades:</td></tr>
<tr><td>R.P8</td><td>Multa:
a) 1% (um por cento) ao dia sobre o valor referente ao respectivo item, no caso de atraso injustificado para a entrega dos equipamentos e do software de gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;
b) 1% (um por cento) ao dia sobre o valor referente aos itens a serem instalados, no caso de atraso injustificado para conclusão do Serviço de Instalação dos Equipamentos e do Software de Gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;
c) Para o item 1, 2% (dois por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 1 (CRÍTICA);
d) Para o item 1, 1% (um por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 2 (ALTA);
e) Para o item 1, 0,5% (meio por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (MÉDIA);
f) Para o item 1, 0,25% (vinte e cinco décimos percentuais) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou</td></tr>
</table>

	solução dos chamados abertos com nível de Prioridade 3 (BAIXA);
R.P9	Os atendimentos às solicitações de severidade crítica, alta ou média deverão ser realizados nas instalações do Contratante (*on-site*) e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo Contratante, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao Contratante;
R.P10	Os atendimentos às solicitações de severidade média poderão ser realizados remotamente ou nas instalações do Contratante (*on-site*), conforme o caso, e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo Contratante, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao Contratante;
R.P11	Os atendimentos às solicitações de severidade baixa poderão ser realizados remotamente, de segunda à sexta-feira, respeitando o horário de funcionamento do Contratante. Caso seja necessário o atendimento nas instalações do Contratante (*on-site*), tal situação não implicará custos adicionais ao Contratante;
R.P12	A interrupção do atendimento de uma solicitação, de quaisquer das severidades, por parte da Contratada sem prévia autorização da Equipe Técnica do Contratante será caracterizada como um descumprimento mensal para efeitos de aplicação dos descontos apresentados no requisito R.P2;
R.P13	Concluído o atendimento, a Contratada comunicará o fato à Equipe Técnica do Contratante e solicitará autorização para o fechamento do chamado. Caso o Contratante não confirme o pleno atendimento da solicitação, o chamado permanecerá aberto até que seja efetivamente atendido. Nesse caso, a Equipe Técnica fornecerá as pendências relativas à solicitação em aberto;
R.P14	O Contratante encaminhará formalmente à Contratada, quando da reunião de apresentação inicial, a relação nominal da Equipe Técnica autorizada a abrir e fechar solicitações de suporte técnico;
R.P15	Todas as solicitações de atendimento serão registradas pelo fiscal do contrato e pela Contratada, para acompanhamento e controle da execução do contrato: a) A Contratada apresentará um Relatório de Atendimento, enviado por meio de correio eletrônico, contendo datas e horas de chamada, de início e de término do atendimento, descrição da necessidade de atendimento, e as providências adotadas e toda e qualquer informação pertinente ao chamado após o encerramento do mesmo; b) A equipe técnica do Contratante informará à Contratada quanto ao recebimento e aceite do Relatório de Atendimento;
R.P16	Na abertura do chamado a Contratada deverá fornecer o número de protocolo e o horário de abertura e encaminhar mensagem de correio eletrônico com tais informações para os endereços dos fiscais do

	contrato em até meia hora após o registro, procedimento que servirá como evidência em caso de contestação de penalidades. O cálculo para aferição da desconformidade do tempo de resposta considerará o tempo de resposta descrito nos níveis mínimos de serviço;
R.P17	Para fins de aferição dos níveis mínimos de serviço, ao final, o chamado será considerado: completamente atendido ou não atendido, não havendo possibilidade de atendimento parcial;
R.P18	Quando a solução depender de ações do Contratante o tempo de solução do chamado deve ser pausado até a conclusão da parte que não cabe a contratada, depois continuar de onde havia parado antes da solicitação do outro ator no processo;
R.P19	Todas as ações provenientes de um chamado deverão ser amplamente comunicadas ao Contratante. Sendo que o Contratante deverá ser comunicado no mínimo em dois momentos, no início e no final de cada atendimento;
R.P20	Os níveis mínimos de serviço serão aferidos mensalmente e eventuais descumprimentos atestados no Termo de Recebimento Definitivo;
R.P21	Toda indisponibilidade causada pela solução contratada, poderá gerar multa de acordo com o NMS descrito acima;
R.P22	Faculta-se à Contratada substituir temporariamente um componente defeituoso por outro de mesmas características técnica ou superior: a) A Contratada deverá realizar a substituição definitiva do referido componente no prazo de 30 (trinta) dias corridos; b) A substituição definitiva de componentes, caso necessário, deverá ser feita por itens novos e para primeiro uso.
R.P23	O Contratante poderá autorizar a substituição, em caráter definitivo, o componente já instalado, por um novo e para primeiro uso, em perfeito estado de funcionamento, no prazo de 30 (trinta) dias corridos, em quaisquer dos seguintes casos: a) Ocorrência de 3 (três) ou mais defeitos que comprometam o seu perfeito funcionamento, dentro de um período qualquer de 30 (trinta) dias corridos; e b) Somatório dos tempos de paralisação de quaisquer componentes que ultrapasse 15 (quinze) horas dentro de um período qualquer de 30 (trinta) dias corridos.
R.P24	Qualquer substituição de componente, temporária ou definitiva, só será permitida após prévia avaliação técnica e autorização por parte da Equipe Técnica do Contratante.

Requisitos de Segurança da Informação	
ID	**Descrição**
R.SI01	O acesso às instalações do Contratante onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas.
R.SI02	A Contratada deverá substituir imediatamente aquele profissional que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares do Contratante.
R.SI03	Os profissionais disponibilizados pela Contratada para a prestação dos

	serviços deverão estar identificados com crachá de identificação da mesma, estando sujeitos às normas internas de segurança do Contratante, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.
R.SI04	A Contratada deverá acatar e obedecer às normas de utilização e segurança das instalações do Contratante.
R.SI05	Respeitar o sistema de segurança do Contratante e fornecer todas as informações relacionadas ao equipamento quando solicitadas por ele.
R.SI06	A Contratada deverá garantir a segurança das informações do Contratante e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do Contratante no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

Requisitos de Garantia	
ID	**Descrição**
R.G1	A garantia será aquela, usualmente fornecida pelo fabricante acrescida dos Níveis de Serviço Exigidos (NSE) e demais condições estabelecidas neste Estudo Técnico;
R.G2	A garantia para todos os equipamentos será de 60 (sessenta) meses.
R.G3	Todos os itens deverão possuir suporte ilimitado para abertura de chamados junto ao Fabricante;
R.G4	A abertura de chamados será efetuada por correio eletrônico e por telefone 0800 ou com número de DDD igual ao da localidade do contratante. Em ambos os casos, o atendimento deve ser efetuado em Língua Portuguesa.
R.G5	O início de atendimento e da resolução do serviço de garantia será a hora da comunicação feita pelo Contratante à Contratada, conforme sistema de registro do próprio do solicitante.
R.G6	Na abertura do chamado, a Contratada deverá fornecer um número de registro para acompanhamento de cada equipamento.
R.G7	O serviço de suporte técnico deverá ser prestado de forma ininterrupta no regime 24x7 (vinte e quatro horas durante sete dias por semana), inclusive em feriados e deverá cobrir todo e qualquer defeito e/ou problema apresentado nos equipamentos ou serviços da solução de *firewall*, peça ou componente, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias.
R.G8	A manutenção será *on-site* (procedimentos realizados no local de instalação) sempre com acompanhamento de um servidor do quadro do Tribunal;
R.G9	Quando não for possível a execução do serviço, em razão da ausência de servidor para acompanhamento, deve o técnico anotar este fato no relatório junto com o tempo de espera;
R.G10	Atualizações para novas versões e releases de *software* lançadas durante a vigência do contrato;
R.G11	Atualizações periódicas de todas as bases de assinaturas dos

	componentes;
R.G12	Suporte para a instalação e configuração das novas versões e *releases* de *software* lançadas durante a vigência do contrato;
R.G13	Apresentação de solução para as solicitações do TST em até 8 (oito) horas, exceto em caso de bug de *software* que deverá ser de 4 (quatro) horas: • Por solução entende-se o atendimento, identificação do problema e sua correção; • Em havendo necessidade de retirada do equipamento para conserto em laboratório, esta deverá substituir o equipamento defeituoso por outro, igual ou superior, em regime 24x7 (vinte e quatro horas durante sete dias por semana), inclusive em feriados com entrega no próximo dia útil, para chamados abertos até às 14h. Após esse horário, o chamado passa a ser contado a partir do próximo dia; • Em caso de defeitos de *software* que necessitem de desenvolvimento de correções pelo fabricante, o prazo deverá ser acordado com o TST;
R.G14	O tempo de indisponibilidade será calculado pela diferença entre a abertura da solicitação e o aceite da correção do problema;
R.G15	Não será considerada indisponibilidade de equipamentos quando ocorrer uma ou mais das seguintes condições: • Quando for caracterizado o uso indevido e/ou mau uso, comprovado por relatório técnico aceito pelo Serviço de Infraestrutura (CITEC); • Quando ocorrer falta de energia elétrica; e • Quando o TST não disponibilizar o equipamento para a manutenção *on-site*, devendo o técnico observar no relatório o tempo de espera. • Quando o Tribunal não disponibilizar técnico para acompanhamento da manutenção.
R.G16	A indisponibilidade cessará quando: • O equipamento for colocado em funcionamento pela Contratada, após testes de validação, acompanhamento e assinatura do Relatório de Atendimento Técnico pelo TST; • O equipamento for substituído por *backup* igual ou superior, quando necessária a retirada para conserto em laboratório; • Equipamentos substituídos por *backup* têm um prazo de 45 (quarenta e cinco) dias corridos para serem devolvidos ao TST, devidamente reparados; • Quando não houver a possibilidade de conserto do equipamento, este deverá ser substituído por equipamento novo, de características iguais ou superiores às do equipamento em questão; • Se o *backup* for um equipamento novo, ele poderá ser aceito na substituição, a critério do TST; • A substituição só será aceita com relatório detalhado sobre as

	causas e motivos do mau funcionamento, assim como a indicação do motivo da impossibilidade de conserto.
R.G17	Substituição de componentes: • Em caso de quebra, mau funcionamento, queda de desempenho ou qualquer outro fato causado por defeitos em componentes dos equipamentos, deverá ser realizado a troca dos componentes por novos, do mesmo modelo ou tecnicamente superiores, homologados pelo fabricante. Não serão aceitos componentes recondicionados ou usados anteriormente.

Poder Judiciário
Justiça do Trabalho
Tribunal Superior do Trabalho

CONTRATO PE-031/2020 – AQUISIÇÃO E INSTALAÇÃO DE SOLUÇÃO DE SEGURANÇA FIREWALL. (Processo TST N.º 501.233/2020-5).

O **TRIBUNAL SUPERIOR DO TRABALHO**, inscrito no CNPJ/MF sob o n.º 00.509.968/0001-48, sediado no Setor de Administração Federal Sul, quadra 8, conjunto A, Brasília, DF, CEP 70070-943, telefone geral (61) 3043-4300, doravante denominado simplesmente **CONTRATANTE**, neste ato representado pelo ....., ..., e a empresa **XXXXXXXXX**, inscrita no CNPJ/MF sob o n.º ....., com sede na ....., Brasília, DF, CEP ....., telefone (xx) ....., e-mail ....., doravante denominada simplesmente **CONTRATADA**, neste ato representada pelo ....., ..., considerando o julgamento do Pregão Eletrônico n.º 031/2020, publicado no Diário Oficial da União do dia xx de xxxxxxx de xxxx, e a respectiva homologação, que consta no Processo Administrativo TST n.º 501.233/2020-5, celebram o presente contrato, observando-se as normas constantes na Lei Complementar n.º 123/2006, nas Leis n.º 8.666/93, 10.520/2002, 8.078/90 e 9.784/99 e nos Decretos n.º 8.538/2015 e 10.024/2019, e ainda, mediante as cláusulas a seguir enumeradas.

CLÁUSULA PRIMEIRA - DO OBJETO

O objeto deste contrato é a aquisição e instalação de solução de segurança para redes de dados do tipo Next Generation Firewall de alta disponibilidade, compreendendo: sistema de detecção e prevenção de intrusão do TIPO IPS/IDS, gerenciamento centralizado e integrado, controle de ameaças, filtro de URL, controle de aplicação, suporte e garantia do fabricante, assinaturas de proteção e suporte técnico em repositório mundial do fabricante, suporte técnico do fabricante local e/ou remoto, incluindo serviços de instalação e treinamento, conforme especificado na tabela abaixo, nos termos e condições constantes neste contrato, seus anexos e no edital.

Item	Especificação	Unidade	Quantidade	Valor unitário/mensal R$	Valor total R$
1	Cluster Firewall NGFW	Equipamento	1		
2	Sistema de Gerenciamento – Next Generation Security Management	Unidade	1		
3	Serviço de Instalação e Configuração	Serviço	1		
4	Treinamento especializado para 5 (cinco) alunos	Turma	1		

Subcláusula primeira. As especificações técnicas do objeto constam no Anexo I deste contrato.

Subcláusula segunda. Os equipamentos deverão ser acondicionados em suas embalagens originais, lacradas e apropriadas para armazenamento, com a sua identificação, fazendo constar sua descrição e incluindo, quando cabíveis: marca, fabricante, data de fabricação, validade e outras especificações de acordo com suas características.

Subcláusula terceira. Do regime de contratação: o objeto do presente instrumento será executado por empreitada por preço global, em conformidade com o disposto na Lei n.º 8.666/1993.

Subcláusula quarta. O prazo de garantia dos equipamentos deste contrato é de, no mínimo, 60 (sessenta) meses contados do recebimento definitivo, conforme o Termo de Garantia do Objeto anexo, que terá vigência independente do prazo de vigência deste contrato.

CLÁUSULA SEGUNDA - DA VIGÊNCIA

O prazo de vigência deste contrato é da data de sua assinatura até cento e vinte dias após o recebimento definitivo do objeto.

CLÁUSULA TERCEIRA - DO VALOR

O valor total deste contrato é de R$ ..... (.....).

Subcláusula única. Já estão incluídas no preço total todas as despesas de impostos, taxas, fretes e demais encargos indispensáveis ao perfeito cumprimento das obrigações decorrentes deste contrato.

CLÁUSULA QUARTA - DO REAJUSTE

Os preços serão fixos e irreajustáveis, nos termos da legislação em vigor.

CLÁUSULA QUINTA - DA DOTAÇÃO ORÇAMENTÁRIA

As despesas oriundas deste contrato correrão à conta dos recursos orçamentários consignados ao Contratante, programa de trabalho ....., elemento de despesa ....., nota de empenho ....., emitida em ...../...../.....

CLÁUSULA SEXTA – DOS PRAZOS

A Contratada deverá cumprir prazo para entrega e instalação dos produtos de, no máximo, 60 (sessenta) dias contados da assinatura deste contrato.

Subcláusula primeira. Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei 8.666/93, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 1 (um) dia do seu vencimento, anexando-se documento comprobatório do alegado pela Contratada.

Subcláusula segunda. Eventual pedido de prorrogação deverá ser encaminhado para o seguinte endereço: Seção de Gestão de Contratos, Tribunal Superior do Trabalho, SAFS, quadra 08, conjunto A, Bloco A, sala T-18, Brasília-DF, CEP 70.070-943, fones: (061) 3043-4096, e-mail: sgcon@tst.jus.br.

Subcláusula terceira. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério do Contratante.

CLÁUSULA SÉTIMA - DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

A execução do objeto deste contrato será fiscalizada por um servidor, ou comissão de servidores, designados pela Administração, doravante denominado Fiscalização, com autoridade para exercer toda e qualquer ação de orientação geral durante a execução contratual.

Subcláusula primeira. São atribuições da Fiscalização, entre outras:

I. acompanhar, fiscalizar e atestar a execução contratual, bem assim indicar as ocorrências verificadas;

II. solicitar à Contratada e a seus prepostos ou obter da Administração todas as providências tempestivas necessárias ao bom andamento do contrato e anexar aos autos cópia dos documentos que comprovem essas solicitações;

III. manter organizado e atualizado um sistema de controle em que se registrem as ocorrências ou os serviços descritos de forma analítica;

IV. notificar a Contratada, por escrito, sobre imperfeições, falhas ou irregularidades constatadas na execução do objeto para que sejam adotadas as medidas corretivas necessárias;

V. propor a aplicação de penalidades à Contratada e encaminhar à Coordenadoria de Material e Logística - CMLOG os documentos necessários à instrução de procedimentos para possível aplicação de sanções administrativas.

Subcláusula segunda. A ação da Fiscalização não exonera a Contratada de suas responsabilidades contratuais.

CLÁUSULA OITAVA - DO RECEBIMENTO E DA ACEITAÇÃO DOS SERVIÇOS E PRODUTOS

O objeto do presente contrato, **relativamente aos itens 1 a 3**, será recebido das seguintes formas:

I. **provisória**, mediante recibo, imediatamente após a entrega dos equipamentos e execução dos serviços, para efeito de posterior verificação de sua conformidade;

II. **definitiva**, mediante recibo, em até dez dias úteis após o recebimento provisório e a verificação da perfeita execução das obrigações contratuais, ocasião em que se fará constar o atesto da nota fiscal.

O **item 4** (treinamento) será recebido da seguinte forma:

I. **provisória**, mediante termo circunstanciado, imediatamente após a entrega da nota fiscal referente aos serviços prestados no mês anterior, para efeito de posterior verificação de sua conformidade;

II. **definitiva**, mediante termo circunstanciado, em até dez dias úteis após o recebimento provisório, a verificação da perfeita execução das obrigações contratuais e mediante a entrega de lista de frequência dos participantes, ocasião em que se fará constar o atesto da nota fiscal.

Subcláusula primeira. Os equipamentos entregues e os serviços prestados em desconformidade com o especificado neste contrato, no instrumento convocatório ou o indicado na proposta serão rejeitados parcial ou totalmente, conforme o caso, e a Contratada será notificada e obrigada a substituí-los e refazê-los a suas expensas, no prazo contratual estabelecido, sob pena de incorrer em atraso quanto ao prazo de execução.

Subcláusula segunda. A notificação referida na subcláusula anterior suspende os prazos de recebimento e de pagamento até que a irregularidade seja sanada.

Subcláusula terceira. Independentemente da aceitação, a Contratada garantirá a qualidade de cada produto fornecido e instalado e estará obrigada a repor aquele que apresentar defeito no prazo estabelecido pelo Contratante.

Subcláusula quarta. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança dos serviços prestados, nem a ético-profissional pela perfeita execução contratual, dentro dos limites estabelecidos pela lei.

CLÁUSULA NONA - DO PAGAMENTO

O pagamento será efetuado em moeda corrente nacional, em até dez dias úteis após o recebimento definitivo, mediante apresentação da nota fiscal devidamente atestada pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

I. o pagamento dos itens 1 e 2 será efetuado após o recebimento definitivo da solução;

II. o pagamento do item 3 será efetuado após o recebimento definitivo dos serviços;

III. para o item 4, os pagamentos serão efetuados mensalmente, em moeda corrente nacional, em até dez dias úteis após o recebimento definitivo de cada mês, mediante apresentação das notas fiscais devidamente atestadas pela Fiscalização, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

Subcláusula primeira. As notas fiscais e os documentos exigidos no edital e neste contrato, para fins de liquidação e pagamento das despesas, deverão ser entregues, exclusivamente, na Coordenadoria de Material e Logística, situada no SAFS, quadra 8, conjunto A, bloco A, térreo, sala T18, CEP 70070-600, Brasília-DF, (61) 3043-4080.

Subcláusula segunda. A Nota Fiscal deverá corresponder ao objeto entregue e respectivos valores consignados na nota de empenho, e a Fiscalização, no caso de divergência, especialmente quando houver adimplemento parcial, deverá notificar a Contratada a substituí-la em até três dias úteis, com suspensão do prazo de pagamento.

Subcláusula terceira. A Contratada deverá entregar todos os produtos e prestar todos os serviços solicitados por meio da nota de empenho e ordem de serviço, não havendo pagamento em caso de entrega parcial até que ocorra o adimplemento total da obrigação.

Subcláusula quarta. A retenção dos tributos não será efetuada caso a Contratada apresente, no ato de assinatura deste contrato, declaração de que é regularmente inscrita no Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas Microempresas e Empresas de Pequeno Porte - Simples Nacional, conforme exigido no inciso XI do art. 4º e modelo constante no anexo IV da Instrução Normativa RFB n.º 1.234, de 11 de janeiro de 2012.

Subcláusula quinta. O Contratante pagará à Contratada a atualização monetária sobre o valor devido entre a data do adimplemento das obrigações contratuais e a do efetivo pagamento, excluídos os períodos de carência para recebimento definitivo e liquidação das despesas, previstos neste contrato, e utilizará o índice publicado pela Fundação Getúlio Vargas que represente o menor valor acumulado no período, desde que a Contratada não tenha sido responsável, no todo ou em parte, pelo atraso no pagamento.

CLÁUSULA DEZ - DAS OBRIGAÇÕES DA CONTRATADA

Na execução deste contrato, a Contratada se obriga a envidar todo o empenho necessário ao fiel e adequado cumprimento dos encargos que lhe são confiados e, ainda, a:

I. entregar os produtos e executar os serviços na forma e em prazo não superior ao máximo estipulado neste contrato;

II. reparar, corrigir, remover e substituir, a suas expensas, as partes do objeto deste contrato em que se verifiquem vícios, defeitos ou incorreções resultantes dos materiais empregados ou da execução dos serviços;

a. a Contratada deverá retirar o material ou componente recusado no momento da entrega do correto.

b. o Contratante não se responsabilizará por qualquer dano ou prejuízo que venha a ocorrer após esse prazo, podendo a Administração dar a destinação que julgar conveniente ao material abandonado em suas dependências.

III. comunicar ao Contratante, por escrito, qualquer anormalidade referente à entrega dos produtos e execução dos serviços, bem como atender prontamente às suas observações e exigências e prestar os esclarecimentos solicitados;

IV. atender prontamente as solicitações da fiscalização do contrato, inerentes ao objeto, sem qualquer ônus adicional para o Contratante;

V. cumprir todos os requisitos descritos no contrato, responsabilizando-se pelas despesas de deslocamento de técnicos, diárias, hospedagem e demais gastos relacionados com a equipe técnica, sem qualquer custo adicional para o Contratante;

VI. respeitar o sistema de segurança do Contratante e fornecer todas as informações solicitadas por ele, relativas ao cumprimento do objeto;

VII. acatar as exigências dos poderes públicos e pagar, às suas expensas, as multas que lhe sejam impostas pelas autoridades;

VIII. guardar inteiro sigilo dos serviços contratados e dos dados processados, bem como de toda e qualquer documentação gerada, reconhecendo serem esses de propriedade e uso exclusivo do Contratante, sendo vedada, à Contratada, sua cessão, locação ou venda a terceiros;

IX. utilizar padrões definidos em conjunto com o Tribunal (nomenclaturas, metodologias, etc.);

X. cumprir os prazos de execução descritos no Anexo I deste contrato;

XI. arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente não seja satisfatório para o atendimento do objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do §1º do art. 57 da Lei nº 8.666/1993;

XII. fornecer, por ocasião da entrega do objeto, a documentação de suporte técnico e manutenção em garantia, contendo as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente, etc.);

XIII. cumprir os requisitos de garantia, bem como os prazos de início de atendimento e de conclusão do reparo do equipamento, descritos no Anexo I deste contrato.

a. O fornecedor deverá assegurar a garantia dos equipamentos, seja por meio da rede mantida pelo próprio fabricante ou por meio de rede por ele credenciada, sendo, em todo caso, capaz de atender no local de entrega dos equipamentos com, no mínimo, um estabelecimento técnico.

b. O término do reparo do equipamento não poderá ultrapassar o prazo previsto; caso contrário, a Contratada deverá providenciar a colocação de equipamento equivalente ou de superior configuração, em perfeitas condições de uso, como backup, até que seja sanado o defeito do equipamento. O prazo máximo para o backup permanecer no Tribunal não deverá ser superior a 30 (trinta) dias, caracterizando, neste caso, a

inexecução total da obrigação, punível com as sanções previstas no caput da cláusula doze.

XIV. manter o Contratante informado quanto a eventuais mudanças de endereço, telefone e e-mail;

XV. manter, durante todo o período de execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas;

XVI. responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, os quais não têm nenhum vínculo empregatício com o TST;

XVII. responder, integralmente, por perdas e danos que vier a causar diretamente ao TST ou a terceiros em razão de ação ou omissão, dolosa ou culposa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita.

Subcláusula primeira. A Contratada não será responsável:

I. por qualquer perda ou dano resultante de caso fortuito ou de força maior;

II. por quaisquer obrigações, responsabilidades, trabalhos ou serviços não previstos neste contrato ou no edital.

Subcláusula segunda. O Contratante não aceitará, sob nenhum pretexto, a transferência de responsabilidade da Contratada para terceiros, sejam fabricantes, representantes ou quaisquer outros.

CLÁUSULA ONZE - DAS OBRIGAÇÕES DO CONTRATANTE

O Contratante, durante a vigência deste contrato, compromete-se a:

I. proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais, inclusive permitir o acesso dos funcionários da Contratada às dependências do TST, relacionadas à execução do objeto deste contrato;

II. promover os pagamentos nas condições e prazo estipulados; e

III. fornecer atestados de capacidade técnica, desde que atendidas as obrigações contratuais. Os requerimentos deverão ser protocolizados ou enviados por correspondência para o Protocolo Geral do TST, localizado no SAFS, quadra 08, conjunto A, bloco A, térreo, Brasília-DF, CEP 70.070-943.

CLÁUSULA DOZE - DAS PENALIDADES SOBRE A CONTRATADA

Fundamentado no artigo 49 do Decreto n.º 10.024/2019, ficará impedido de licitar e contratar com a União e será descredenciado no SICAF, pelo prazo de até 5 (cinco) anos, garantido o

direito à ampla defesa, sem prejuízo das multas previstas no edital, neste contrato e das demais cominações legais, aquele que:

I. não entregar documentação exigida neste contrato;
II. apresentar documentação falsa;
III. causar o atraso na execução do objeto;
IV. não mantiver a proposta;
V. falhar ou fraudar na execução contratual;
VI. comportar-se de modo inidôneo;
VII. declarar informações falsas;
VIII. cometer fraude fiscal.

Subcláusula primeira. O atraso injustificado na execução contratual implicará multa correspondente a 0,5% (cinco décimos por cento) por dia de atraso, calculada sobre o valor do objeto em atraso, até o limite de 15% (quinze por cento) do respectivo valor total.

Subcláusula segunda. Na hipótese mencionada na subcláusula anterior, o atraso injustificado por período superior a 30 (trinta) dias caracterizará o descumprimento total da obrigação, punível com a sanção prevista no *caput* desta cláusula, como também a inexecução total do contrato.

Subcláusula terceira. Durante a execução do contrato, caso existam ocorrências que ultrapassem os níveis de tolerância informados nos requisitos de prazo do Anexo I, serão aplicadas multas, detalhadas a seguir:

a. 1% (um por cento) ao dia sobre o valor referente ao respectivo item, no caso de atraso injustificado para a entrega dos equipamentos e do software de gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;
b. 1% (um por cento) ao dia sobre o valor referente aos itens a serem instalados, no caso de atraso injustificado para conclusão do Serviço de Instalação dos Equipamentos e do Software de Gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato;
    i. Para o item 1, 2% (dois por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 1 (CRÍTICA);
    ii. Para o item 1, 1% (um por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 2 (ALTA);
    iii. Para o item 1, 0,5% (meio por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos

para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (MÉDIA);

iv. Para o item 1, 0,25% (vinte e cinco décimos percentuais) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (BAIXA).

Subcláusula quarta. Poderão ser aplicadas subsidiariamente as sanções de advertência, suspensão e declaração de inidoneidade previstas nos artigos 86 e 87 da Lei n.º 8.666/93.

Subcláusula quinta. A penalidade de multa prevista nas subcláusulas primeira a terceira poderá ser substituída pela penalidade de advertência, tendo em vista as circunstâncias da execução contratual, garantida a prévia defesa, na forma da lei.

Subcláusula sexta. As multas porventura aplicadas serão descontadas dos pagamentos devidos pelo Contratante ou cobradas diretamente da Contratada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

Subcláusula sétima. As penalidades serão obrigatoriamente registradas no SICAF, e a sua aplicação será precedida da concessão da oportunidade de ampla defesa para a Contratada, na forma da lei.

CLÁUSULA TREZE - DAS CONDIÇÕES DE HABILITAÇÃO DA CONTRATADA

A Contratada declara, no ato de celebração deste contrato, estar plenamente habilitada à assunção dos encargos contratuais e assume o compromisso de manter, durante a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação.

CLÁUSULA QUATORZE - DA PUBLICAÇÃO

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 QUINZE - DAS ALTERAÇÕES DO CONTRATO

Compete a ambas as partes, de comum acordo, salvo nas situações tratadas neste instrumento, na Lei n.º 8.666/93 e em outras disposições legais pertinentes, realizar, via termo aditivo, as alterações contratuais que julgarem convenientes.

CLÁUSULA DEZESSEIS - DA RESCISÃO

Constituem motivos incondicionais para rescisão do contrato as situações previstas nos artigos 77 e 78, na forma do artigo 79, inclusive com as consequências do artigo 80, da Lei n.º 8.666/93.

CLÁUSULA DEZESSETE - DA UTILIZAÇÃO DO NOME DO CONTRATANTE

A Contratada não poderá, salvo em curriculum vitae, utilizar o nome do Contratante ou sua qualidade de Contratada em quaisquer atividades de divulgação profissional como, por exemplo, em cartões de visita, anúncios diversos, impressos etc., sob pena de imediata rescisão deste contrato.

Subcláusula única. A Contratada não poderá, também, pronunciar-se em nome do Contratante à imprensa em geral sobre quaisquer assuntos relativos às atividades deste, bem como a sua atividade profissional, sob pena de imediata rescisão contratual e sem prejuízo das demais cominações cabíveis.

CLÁUSULA DEZOITO - DOS CASOS FORTUITOS, DE FORÇA MAIOR OU OMISSOS

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.

CLÁUSULA DEZENOVE - DAS DISPOSIÇÕES FINAIS

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.

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

Subcláusula segunda. Os agentes públicos responderão, na forma da lei, por prejuízos que, em decorrência de ação ou omissão dolosa ou culposa, causarem à Administração no exercício de atividades específicas do cumprimento deste contrato, inclusive nas análises ou autorizações excepcionais constantes nestas disposições finais.

Subcláusula terceira. 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.

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

Subcláusula quinta. No curso do contrato, é admitida a fusão, cisão ou incorporação da empresa, bem assim sua alteração social, modificação da finalidade ou da estrutura, desde que não prejudique a execução do contrato, cabendo à Administração decidir pelo prosseguimento ou rescisão do contrato.

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

Subcláusula sétima. Em consonância com a Resolução 229, de 22 de junho de 2016, do Conselho Nacional da Justiça, é vedada a contratação de empresas 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.

I. A vedação constante nesta subcláusula se estende às contratações cujo procedimento licitatório tenha sido deflagrado quando os magistrados e servidores geradores de incompatibilidade estavam no exercício dos respectivos cargos e funções, assim como às licitações iniciadas até 6 (seis) meses após a desincompatibilização.

CLÁUSULA VINTE - DO FORO

Fica eleito o foro da cidade de Brasília, DF, como competente para dirimir quaisquer questões oriundas deste contrato, com exclusão de qualquer outro, por mais privilegiado que seja.

E, por estarem ajustadas e acordadas, as partes assinam este termo em duas vias de igual teor e forma para um só efeito legal.

Brasília, de de 201 .

CONTRATANTE **CONTRATADA**

Poder Judiciário
Justiça do Trabalho
Tribunal Superior do Trabalho

ANEXO I

Requisitos Tecnológicos (hardware e software)	
ID	**Descrição**
R.HS1	Para efeitos deste Estudo Técnico, o uso das conjunções "e/ou" deve ser compreendido de forma ampla, ou seja, deve ser considerada a possibilidade de os elementos serem tomados em conjunto e, também, separadamente. Por exemplo, a expressão "Controle de políticas por porta e/ou protocolo" deve ser compreendida da seguinte forma: "O parâmetro para aplicação de políticas deve ser aplicado: a) por porta individualmente; b) por protocolo individualmente; e c) por porta e protocolo simultaneamente";
R.HS2	Cada solução de alta disponibilidade deverá ser composta por 2 (dois) equipamentos (*appliances*) funcionando em *cluster*, construídos especificamente para exercer a função de *Next Generation Firewall*, com *hardware* e *software* fornecidos pelo mesmo fabricante.
R.HS3	Deverá ser fornecida com licença(s) do(s) *software*(*s*) embutido(s) em todos os seus componentes, ou seja, durante a vigência da garantia, todas as atualizações deverão ser disponibilizadas ao Contratante. Após o seu término, a Contratante poderá continuar a utilizar o *firewall*, sem as funcionalidades de NGFW;
R.HS4	Deverá ser licenciado e habilitado para uso ilimitado de usuários e endereços IP;
R.HS5	Deverá possuir ao menos as seguintes funcionalidades nativas, que deverão operar na mesma solução: • *Firewall*; • Controle de Aplicação; • Gerenciamento de Qualidade de Serviço (QoS); • Prevenção contra Ameaças (IPS, *BotNets*); • Proteção contra Ameaças Avançadas; • Identificação de Usuários; • Filtro de URL; • Rede VPN; • Console de Gerenciamento e Monitoramento;
R.HS6	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
R.HS7	Será aceita somente solução com as funcionalidades nativas descritas no item R.HS5 instaladas em ambiente físico local (*on-premise*), sendo vedada qualquer transmissão de informação para processamento na nuvem, exceto para atualização da base de dados da solução e prevenção contra ameaças avançadas;
R.HS7.1	Com relação à Proteção contra Ameaças Avançadas, poderá ser entregue equipamento físico exclusivo para essa finalidade com processamento local dos arquivos ou, caso a solução seja baseada em tratamento de dados na nuvem, essa deverá ser capaz de processar os arquivos definidos pela Contratante, independente do volume mensal, e agregar a proteção do tipo "*zero day*" par quaisquer situações;
R.HS8	Deve executar funcionalidades de proteção de rede, proteção e prevenção contra ameaças avançadas e não conhecidas, e somente será aceita solução (*hardware* e *software*) de um mesmo fabricante;

R.HS9	O *software* deverá ser fornecido em sua versão mais atualizada, relativo à data de sua instalação e configuração, não sendo permitido qualquer tipo de comprovação futura;
R.HS10	O *hardware* deve ser baseado em arquitetura que garanta flexibilidade e adaptação a novas ameaças sem impacto no desempenho;
R.HS11	A comunicação entre a solução de gerência e a solução de *hardware* de segurança, deverá ser criptografada;
R.HS12	Deve ser possível suportar arquitetura de armazenamento de *logs* redundante, permitindo a configuração de equipamentos distintos;
R.HS13	Possuir mecanismo de indexação de *logs* para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de *logs* mais antigos;
R.HS14	Os *gateways* de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;
R.HS15	Oferecer a funcionalidade de *backup*, assim como permitir ao administrador agendar procedimentos de *backups* periódicos;
	HARDWARE
R.HS16	Armazenamento de no mínimo de 1TB com 2 (dois) discos em RAID1, por equipamento, pois a falha do disco, se único, ocasionará indisponibilidade da solução bem como os dados de *log* nele existentes; • Caso a solução ofertada possua recurso de replicação síncrona de todos os dados para a solução de gerência, está será aceita.
R.HS17	Memória suficiente ou outra arquitetura que garanta desempenho sempre inferior a 75% de utilização da solução durante toda a vigência contratual; • O monitoramento poderá ser realizado tanto pelo sistema de gerenciamento centralizado ou por ferramenta própria de monitoração do TST, com intervalos mínimos de 5 minutos entre cada aferição.
R.HS18	Todos os equipamentos e seus componentes deverão ser novos, sem uso, entregues em perfeito funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.
R.HS19	Não serão aceitos equipamentos em modo *End of Life, End of Sale* e *End of Support*.
R.HS20	Mínimo de 4 (quatro) interfaces do tipo 10/100/1000 base-T RJ45 ou superior, com os respectivos *tranceivers*, para cada equipamento do *cluster*;
R.HS21	Mínimo de 4 (quatro) interfaces de rede do tipo 10Gbps SFP+, com os respectivos *tranceivers* bidirecional, com conector LC, para cada equipamento do *cluster*;
R.HS22	Mínimo de 4 (quatro) interfaces tipo 40Gbps QSFP+ bidirecional, com os respectivos *tranceivers* com conector LC, para cada equipamento do *cluster*;
R.HS23	Mínimo de 1 (uma) interface, dedicada para gerenciamento;
R.HS24	Mínimo de 1 (uma) interface, dedicada para console;
R.HS25	Mínimo de 1 (uma) interface, dedicada para sincronismo do *cluster*;
R.HS26	Mínimo de 1 (uma) interface, dedicada para gerenciamento *out-of-band*;
R.HS27	Fonte de alimentação 120/240 VAC, redundante e *hot-swappable*;
R.HS28	Ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 90% (sem condensação) e temperatura ambiente na faixa de 0°C a 40°C.
R.HS29	Vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos, etc.) para fixação em bastidor (*rack*) padrão EIA-310 com largura de 19"(dezenove polegadas).

Poder Judiciário
Justiça do Trabalho
Tribunal Superior do Trabalho

R.HS30	Possuir certificação de conformidade sustentável de acordo com os padrões EPA (*Enviromental Protection Agency*) ou similar, tais como, *EnergyStar*, *RoHS* (*Restriction on Harzadous Substances*), WEEE (*Waste Electrical and Eletronic Equipament*) ou EMI *Certifications* FCC *part* 15, CE, EN55022, EN55024.
R.HS31	Possuir *throughput* de proteção de, no mínimo, 15 (quinze) Gbps para as funcionalidades de *firewall*, Controle de Aplicação, Prevenção de Ameaças (IPS, *BotNets* e Antivírus), Proteção contra Ameaças Avançadas, Filtro de URL, Identificação de Usuários da Solução, Características de *QoS*, características de VPN habilitadas simultaneamente;
R.HS31.1	O *throughput* é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Caso a fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado.
R.HS32	Suportar, no mínimo, 8.000.000 (oito milhões) de conexões concorrentes;
R.HS33	Suportar, no mínimo, 200.000 (duzentos mil) novas conexões por segundo;
R.HS34	As taxas de transferência indicadas devem ser alcançadas com a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, sem prejuízo no desempenho do equipamento, e com todas as assinaturas, lista e demais métodos de controle de acesso e de detecção e prevenção de ameaças habilitados;

	FIREWALL
R.HS35	Suportar os protocolos IPv4 e IPv6;
R.HS36	Suportar no mínimo 1024 VLANs no padrão 802.1q e estabelecer regras de filtragem (*Stateful Firewall*) entre elas;
R.HS37	Suportar agregação de *links* no padrão 802.3ad;
R.HS38	Suportar *policy based routing* ou *policy based forwarding*, possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;
R.HS39	Suportar roteamento *multicast* (PIM-SM);
R.HS40	Suportar DHCP *Relay* e DHCP *Server*;
R.HS41	Suportar *jumbo frames*;
R.HS42	Suportar NAT dinâmico (N-to-1 e N-to-N);
R.HS43	Suportar NAT estático (N-to-1 e N-to-N);
R.HS44	Suportar NAT estático bidirecional (1-to-1);
R.HS45	Suportar tradução de porta (PAT);
R.HS46	Suportar NAT de origem e NAT de destino, simultaneamente;
R.HS47	Enviar *log* para sistemas de monitoramento externos, simultaneamente aos registros internos;
R.HS48	Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (*anti-spoofing*) para IPv4;
R.HS49	Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
R.HS50	Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
R.HS51	Suportar OSPF *graceful restart*;
R.HS52	Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente e em *layer* 3;
R.HS53	Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: • Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 e camada 3; • Modo *sniffer*, para inspeção via porta espelhada do tráfego de dados da rede; • Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; • Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como *default gateway* das redes protegidas; • Modo Misto de trabalho *sniffer*, L2 e L3, em diferentes interfaces físicas.
R.HS54	A configuração em alta disponibilidade deverá ser implantada de forma a suportar *clusters* ativo/ativo e ativo*/standby*, devendo sincronizar: • Sessões; • Configurações, incluindo, mas não limitado a políticas de *firewall*; • NAT e objetos de rede; • Associação de Segurança das VPNs; • Tabelas FIB; • Tabelas de usuários autenticados.
R.HS55	O HA deve possibilitar monitoramento de falha de *link*;
R.HS56	Suportar atuação como cliente NTP (*network time protocol*);

	CONTROLE POR POLÍTICAS DE SEGURANÇA
R.HS57	A solução de segurança deve usar *Stateful Inspection* baseada na análise de comunicação e de estado da conexão para monitorar e controlar o fluxo de rede;
R.HS58	Permitir a implementação de monitoramento do seguimento de Internet, através de teste de conectividade com endereços específicos, e implantar alertas em caso de quedas; • Os alertas poderão ser implementados via API.
R.HS59	As regras deverão ser elaboradas utilizando objetos de rede baseados em TCP/IP. Durante a criação da regra, tais objetos deverão ser associados sem que haja necessidade de associação à interface de rede de origem ou destino da conexão ou então permitir a configuração para todas as interfaces simultaneamente;
R.HS60	Possibilitar a configuração, entre os nós do *cluster*, no mínimo, nos modos Ativo/Ativo e Ativo/*Standby*, garantindo assim, que apenas um dos nós consiga suportar toda a demanda dessa especificação técnica;
R.HS61	Após uma queda ou reconexão de qualquer dos *links*, deve ser possível configurar ações como alertas SNMP, armazenamento do *log scripts* customizados pelo usuário;
R.HS62	Autenticar sessões ou usuários para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;
R.HS63	Controles de políticas por porta e/ou protocolo;
R.HS64	Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
R.HS65	A base de categorias e aplicações deve ser fornecida e constantemente atualizada pelo fabricante da solução, sempre que uma alteração em sua base seja feita. Deve permitir, ainda, que algum objeto seja sobrescrito por configuração do próprio administrador;
R.HS66	Controle de políticas por usuários, grupos de usuários, IPs, redes e/ou grupos de redes;
R.HS67	Controle de políticas por código de Países, sem que seja necessário configurar manualmente o escopo de endereço desses países;
R.HS68	Suportar a criação de políticas por geolocalização, permitindo que o tráfego de entrada e/ou de saída de determinado(s) país(es) seja(m) bloqueado(s);
R.HS69	Deve decriptografar tráfego *inbound* e *outbound* em conexões negociadas com, no mínimo, TLS 1.1 e TLS 1.2;
R.HS70	Bloqueio dos seguintes tipos de arquivos como *bat, cab, dll, exe, pif* e *reg* e outros, de acordo com a necessidade, configuráveis através do *software* de gerência disponibilizado;
R.HS71	*Traffic shapping* e *QoS* – priorização de tráfego de dados baseada em Políticas (Prioridade, Garantia e Limitação máxima);
R.HS72	Suporte a configuração de regras que permitam informar endereço IP nas versões IPv4 e IPv6, sem duplicação de regra;
R.HS73	Suporte a objetos e regras *multicast*;
R.HS74	Permitir o agendamento de aplicação automática de políticas em horário pré-definidos pelos administradores;
R.HS75	Deve suportar importação de certificado em inspeção de conexões SSL de entrada (*inbound*);

R.HS76	A solução deve ser capaz de identificar o comportamento do protocolo SSH, onde pode ser feito através de padrões de análise de protocolo;
R.HS77	Deve ter a capacidade de inspecionar e bloquear tráfego operando em camada 2 e camada 3;
R.HS78	Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações;
R.HS79	Deve inspecionar e bloquear os dados operando como *default gateway* das redes protegidas e controlar o tráfego em nível de aplicações;
R.HS80	Na ocorrência de falhas, as conexões existentes em um *firewall* deverão ser mantidas pelo(s) outro(s), sem perdas destas conexões, não acarretando interrupções no tráfego da rede e nem redução de desempenho da solução;
R.HS81	Na aplicação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas;
R.HS82	Promover a integração com diretório LDAP (X.500) e *Active Directory* para a autenticação de usuários, de modo que o *Firewall* possa utilizar das informações armazenadas para realizar autenticações;
R.HS83	Para configuração a administração do *Firewall* deve possibilitar o acesso via CLI (SSH), console do fabricante e interface *web* HTTPS;
R.HS84	A solução de *Firewall* deve prover funcionalidade que permita visualização do grau de utilização de cada regra, por exemplo, quantidade de *hits* por regra, % de utilização ou volume em *bytes*;
R.HS85	A solução deve, por padrão, não permitir que ataque do tipo "*scan ports*" ou similares retornem resultados do estado das portas;
R.HS86	A solução de *Firewall* deve suportar no mínimo, 10.000 (dez mil) regras;
R.HS87	A solução deve suportar o mínimo de 16.384 entradas de endereço ARP;
R.HS88	Deverá permitir a aceleração e otimização da leitura das regras, de modo que o *firewall* consiga identificar padrões muito utilizados;
R.HS89	Deverá suportar métodos de autenticação de, no mínimo, usuário e cliente;
R.HS90	A solução deverá disponibilizar interface para gerenciamento das atualizações de segurança para instalação agendada ou automática, conforme determinação da Contratante;
	CONTROLE DE APLICAÇÕES
R.HS91	A solução deverá contar com ferramentas de visibilidade e controle de aplicações *web* integradas na própria solução de segurança, que permitam a criação de políticas de liberação ou bloqueio baseando-se em aplicações *web* 2.0;
R.HS92	Deve prover o controle e a proteção de acesso à Internet por meio do reconhecimento das aplicações *web 2.0*, independente de porta e protocolo, e da classificação de URL's;
R.HS93	Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
R.HS94	Deve ser capaz de identificar um mínimo de 2.000 (duas mil) aplicações, incluindo, mas não se limitando a: *peer-to-peer*, *streaming* de áudio e vídeo, *update* de *software*, *instant messaging*, redes sociais, *proxies*, *anonymizers*, acesso e controle remoto, VoIP e e-mail;
R.HS95	Deve ser capaz de identificar, no mínimo, as seguintes aplicações: *BitTorrent*, *Youtube*, *Livestream*, *Skype*, *Viber*, *WhatsApp*, *Snapchat*, *Facebook*, *Facebook Messenger* ou *Facebook Chat*, *G Suite*, *Tinder*, *Instagram*, *Twitter*, *Linkedin*, *Dropbox*, *One* Drive ou *Microsoft One Drive*, *Logmein*, *TeamViewer*, MS-RDP, VNC, *Ultrasurf*, TOR, *Webex*, *Evernot*, *Amazon Cloud Drive*, *Gotomeeting*.

R.HS96	Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, *social widgets* (ou similar) com controle granular para usuários ou grupos de usuários;
R.HS97	A solução deverá possuir pelo menos as categorias de aplicações *web* pré-definidas pelo fabricante, atualizadas em tempo real;
R.HS98	Deve possibilitar a inspeção de tráfego HTTPS (*inbound/outbound*);
R.HS99	Deve ser capaz de identificar aplicações criptografadas usando SSL;
R.HS100	Deve possibilitar o bloqueio das aplicações, de portas e protocolos;
R.HS101	Deve possibilitar a criação de regras com várias categorias;
R.HS102	Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reiniciar os *gateways* e gerência;
R.HS103	Deve possibilitar a permissão ou bloqueio de aplicações por, pelo menos, os seguintes critérios: • Aplicação da *web*; • Categorias; • IP/Range de IP's/Redes; • Usuários do AD/LDAP; • Grupos de usuários do AD/LDAP; • Aplicações tais como *Ultrasurf*, *Torrent*, *Dropbox* e demais *File Sharing.*
R.HS104	Deve possibilitar a customização da tela de interação com o usuário, permitindo: • Informar sobre o bloqueio; • Questionar sobre a necessidade de acesso. •
R.HS105	Deve possibilitar a customização de regra utilizando as seguintes ações de controle: • Permitir; • Bloquear; • Bloquear e informar; • Monitorar; • Informar o usuário.
R.HS106	Deve permitir o bloqueio total de aplicações do tipo *proxy* (*Ultrasurf, Tor, etc.*);
R.HS107	Deve possibilitar a integração da solução com base do *Microsoft Active Directory*, LDAP, RADIUS ou base local para criação de políticas utilizando: • Usuários; • Grupo de Usuários; • Objetos cadastrados vinculados ao endereço IP; • Endereço IP; • Endereço de Rede; • Combinação das opções acima.
R.HS108	A solução deve suportar a criação de pelo menos 600 regras de controle de aplicações no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso;
R.HS109	O mecanismo de Controle de aplicação *Web*/URL deve apresentar contagem de utilização de regra de acordo com a utilização;
R.HS110	A solução deve ter um mecanismo configurável de *by-pass*, onde o administrador consegue definir grupos específicos de usuários ou de máquinas que estão autorizados a ignorar as regras de inspeção SSL;
R.HS111	Deverá categorizar as aplicações ou URL's por fator de risco;

R.HS112	A solução deverá receber atualizações, para sua base de aplicações e URL's, a partir de um serviço baseado em nuvem, fornecido pelo fabricante da solução;
R.HS113	A solução deverá possuir uma console gráfica centralizada para gerenciar regras de *firewall*, de aplicações e de URL's;
R.HS114	Deverá possuir um mecanismo para informar ou perguntar ao usuário, em tempo real, com a finalidade de educa-los ou confirmar ações baseadas na política de acesso;
R.HS115	Deverá permitir a criação de exceções baseadas em objetos de rede;
R.HS116	A solução deve prover a opção de editar a notificação de bloqueio e redirecionar o usuário para a página de remediação;
R.HS117	Deve incluir o mecanismo de *black list* e *white list* permitindo ao administrador do sistema negar ou permitir o acesso a determinadas URL's, independente da categoria;
R.HS118	Deve inspecionar o *payload* do pacote de dados com o objetivo de detectar, através de expressões regulares (ou similar), assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não se limitando ao uso de protocolo *Remote Desktop Protocol* na porta 80 ao invés da porta 3389;
R.HS119	Para tráfego criptografado (SSL), deve decriptografar pacotes a fim de possibilitar a leitura do *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;
R.HS120	Deve realizar a decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
R.HS121	A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não se limitando a compartilhamento de arquivo de soluções;
R.HS122	Deve detectar arquivos e outros conteúdos que devem ser inspecionados de acordo com as regras de segurança implementadas em outras camadas;
R.HS123	Identificar o uso de técnicas evasivas através de comunicações criptografadas;
R.HS124	Limitar a banda (*download/upload*) usada por aplicações baseado no IP de origem, usuários e grupos do LDAP/AD;
R.HS125	Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário d rede em tempo real com integração ao *Microsoft Active Directory*, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários;
R.HS126	Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
R.HS127	Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do TST;
R.HS128	O fabricante deve permitir a solicitação de inclusão ou alteração de categorização na base de assinaturas das aplicações;
R.HS129	Deve alertar o usuário quando uma aplicação for bloqueada;
R.HS130	Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
R.HS131	Deve possibilitar a diferenciação de tráfego de *Instant Messaging* possuindo granularidade de controle e/ou políticas;

R.HS132	Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o *Whatsapp* e bloquear a transferência de arquivos;
R.HS133	Deve permitir a criação de regras de liberação e bloqueio utilizando apenas o domínio, usando expressões regulares, sem necessidade de inserção do endereço IP pelo administrador, onde a resolução deve ser feita de forma automática e em tempo real pela solução, inclusive para consultas baseadas em nuvem.
R.HS134	Deve ser possível a criação de grupos estáticos e dinâmicos de aplicações;
	PREVENÇÃO DE AMEAÇAS
R.HS135	Deve incluir assinaturas de prevenção de intrusão, IPS, e suporte ao bloqueio de arquivos e códigos maliciosos;
R.HS136	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar: *Antivírus*, *Antimalware* e *BotNets* integrados na própria solução de *firewall* sem a necessidade de uso de quaisquer interfaces externas, onde sua console de gerência deverá residir na mesma console centralizada;
R.HS137	Deve sincronizar as assinaturas de prevenção de ameaças por demanda ou por agendamento;
R.HS138	As assinaturas devem permitir a ativação e desativação, ou ainda, ativação apenas em modo de monitoramento;
R.HS139	Exceções por IP de origem ou destino devem ser possíveis, de forma geral e assinatura-a-assinatura;
R.HS140	Deve suportar granularidade nas políticas de *Antivírus* e *Antimalware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, grupo de usuários, serviço ou assinatura e a combinação de todos esses itens;
R.HS141	Deve suportar o bloqueio de vulnerabilidades;
R.HS142	Deve incluir proteção contra ataque de negação de serviços (*DoS* e *DDoS*);
R.HS143	Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos os seguintes ataques conhecidos: SQL *Injection*, ICMP *denial of servisse*, força bruta e *port scanner*, SMB, *Port overflow*, *Non compliant* SSL;
R.HS144	Deverá possuir mecanismos de detecção de assinaturas, anomalias de protocolos, controle de aplicações e detecção de comportamento;
R.HS145	A solução de IPS deve fazer a inspeção de toda a sessão, independentemente do tamanho, de forma bidirecional, sem degradas o desempenho do equipamento;
R.HS146	O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar a solução;
R.HS147	Deve estar incluso informações como código CVE (*Common Vulnerabilities and Exposures*), severidade e tipo de ação a ser executada em cada proteção de segurança, mesmo que de forma manual;
R.HS148	Deve ser capaz de bloquear tráfego SSH enviado em portas diferentes da porta padrão;
R.HS149	As regras de exceção deverão possuir origem, destino, serviço, severidade, grupo de usuário ou alguma dessas combinações;
R.HS150	A solução deve ser capaz de inspecionar tráfego HTTPS de entrada e saída;
R.HS151	A solução de IPS integrada na solução de segurança deve possuir uma base de assinatura não inferior a 10.000 (dez mil) assinaturas;

R.HS152	A solução de IPS deve possuir funcionalidade que permita configurar as assinaturas do IPS o modo apenas de detecção para fins de *troubleshooting*;
R.HS153	A solução de IPS deve possuir índices por período que apontem o nível de ação das assinaturas baseado pela sua severidade na própria interface de gerência;
R.HS154	A solução deve permitir incorporar de forma automática novas proteções de IPS através de sua severidade;
R.HS155	O módulo de IPS deve possuir assinaturas voltadas para ambiente de servidores *web* e DNS;
R.HS156	A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação protegendo, pelo menos, os seguintes serviços: Aplicações *web*, serviços de e-mail, DNS, FTP, serviços *Windows* (*Microsoft Networking*) e VoIP;
R.HS157	A solução deve permitir ao administrador configurar quais métodos e comandos HTTP e comandos FTP são permitidos e quais são bloqueados;
R.HS158	Deve incluir proteção contra vírus e *worms* em conteúdo *ActiveX*, *applets Java* e outros;
R.HS159	Deve possuir perfis pré-configurados de proteção de IPS que podem ser utilizados a qualquer momento;
R.HS160	Deve incluir tela de visualização a fim de monitorar graficamente a quantidade de alertas de diferentes severidades. As diferentes áreas de interesse devem ser definidas utilizando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades da solução, incluindo pelo menos: origem, destino, serviço, usuário, tipo e nome do alerta;
R.HS161	A solução deve permitir a configuração de inspeção do IPS baseada em políticas que utilizem o posicionamento geográfico de origens ou destinos e combinações entre os dois;
R.HS162	A solução de possuir esquemas de atualização de assinaturas, no mínimo, através de agendamento, modo *off-line* e por demanda;
R.HS163	A solução deverá possuir relatório e correlação de eventos centralizada;
R.HS164	A solução deverá permitir a ativação de novas proteções baseada em parâmetros configuráveis como: severidade da ameaça, proteções para clientes e proteções para servidores;
R.HS165	A solução deve proteger contra ataques do tipo DNS *Cache Poisoning* e impedir que os usuários acessem endereços de domínios bloqueados;
R.HS166	A solução deve permitir bloquear o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente o *range* de endereços IP dos países que se deseja bloquear;
R.HS167	Ser imune e capaz de impedir ataques básicos como: SYN *flood*, ICMP *flood*, UDP *flood*;
R.HS168	Suportar análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
R.HS169	A solução deverá realizar análise de *malware,* em sistemas físicos exclusivos (*bare metal*), evitando a atuação de *malwares* que reconheçam sistemas de *sandbox*;
R.HS170	Deverá ser capaz de decriptografar para análise pelo menos os protocolos SSL;
R.HS171	Deverá ser capaz de implementar autenticação para aplicações de multifator (MFA) ;
R.HS172	Detectar e bloquear a origem de *port scans*;
R.HS173	Possuir assinaturas para bloqueio de ataques de *buffer overflow*;
R.HS174	Suportar o bloqueio de vírus e *spywares*;

R.HS175	Suportar bloqueio de arquivos por tipo ou extensão;
R.HS176	Identificar e bloquear comunicação com *BotNets*;
R.HS177	Deve suportar referência cruzada com CVE (*Common Vulnerabilities and Exposures*);
R.HS178	A solução deve possuir nuvem de inteligência proprietária do fabricante, que seja responsável em atualizar toda a base de segurança do *appliances* através de assinaturas, durante a vigência do contrato;
R.HS179	Implementar modo de configuração totalmente transparente para o usuário final de modo que não haja necessidade de configuração de *proxies*, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
R.HS180	Implementar funcionalidade de detecção e bloqueio de *call-backs* (comunicação do *malware* com o servidor de comando e controle);
R.HS181	A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede, baseado em análises de tráfego de rede, processamento de pacotes, dentre outros;
R.HS182	A solução de proteção contra *BotNets* deve utilizar mecanismo de detecção em multicamadas, que inclui reputação ode endereço IP, URLs e endereços DNS, assim como detecção de padrões de comunicação BOT;
R.HS183	O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regras individuais visando aperfeiçoar o desempenho do equipamento;
R.HS184	A solução de segurança deve permitir o bloqueio de *download* de arquivos que exceda tamanho pré-definido;
R.HS185	A solução deve analisar e bloquear *malwares* e/ou códigos maliciosos pelo menos nos seguintes tipos de arquivos do pacote *office* (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), MacOS (*mach*-O, DMG e PKG), *Linux* (ELF), RAR e 7-ZIP, análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL;
R.HS186	A solução deve realizar a análise dos arquivos de *download* anteriormente a entrega ao usuário;
R.HS187	Possuir antivírus em tempo real para ambiente de *gateway* internet, integrado à plataforma de proteção para os protocolos HTTP, HTTPS e SMTP;
R.HS188	A solução deve atuar na prevenção de forma granular através de políticas por usuário/máquina ou rede, sendo possível escolher um perfil diferente para cada regra ou prover todas as informações necessárias no *log* para a criação da exceção de forma manual;
R.HS189	A solução deve permitir criar regras de exceção de acordo com a proteção a partir do *log* visualizado na interface gráfica da gerência centralizada;
R.HS190	A solução de relatório deve apresentar via interface gráfica, no mínimo, informações de *hosts* infectados, atividades de *malware* e detalhes dos alertas;
R.HS191	Deve possuir visualização na própria interface de gerência dos maiores incidentes através de *hosts* ou incidentes de vírus e *bots*;
R.HS192	A solução deve permitir compartilhar informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do fabricante;
R.HS193	Permitir o bloqueio de *malwares*;
R.HS194	A solução deverá ser capaz de manter a análise de antivírus em caso de falha de conexão com a nuvem, bem como permitir criação de regras exceção para análise de antivírus;
R.HS195	A solução deverá possuir mecanismo para proteger contra ataques de *phishing*;

R.HS196	A solução deve ser capaz de proteger contra ataques DNS, tais como capacidade de detectar e prevenir C&C DNS *Hide Out*, analisar padrões de comunicação C&C e não apenas o servidor DNS de destino, realizar engenharia reversa do *malware*, detecção passiva de DNS e de comando e controle (C&C) e capacidade para detectar e prevenir ataques DNS *tunneling*;
R.HS197	A solução deverá suportar análise de arquivos que trafegam dentro do protocolo SMB, versões 2 e 3;
R.HS198	Deve suportar a inspeção em arquivos compactados;
	PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS
R.HS199	A solução deverá prover as funcionalidades de inspeção de tráfego de entrada de *malwares* não conhecidos (APT *Advanced Persistent Threat* e *Zero-Day Threats*), *ransomwares* com filtro de ameaças avançadas e análise de execução em tempo real e inspeção de tráfego de saída de *call-backs*;
R.HS200	Possuir capacidade de prevenção de ameaças não conhecidas;
R.HS201	A solução deve possuir funcionalidades para prevenção de *malwares* não conhecidos, incluídas na própria ferramenta (*zero-day*);
R.HS202	Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP;
R.HS203	Deve ser capaz de inspecionar tráfego criptografado usando SSL;
R.HS204	A solução deve possuir mecanismo para identificar *hosts* infectados tentando acessar endereços de DNS de domínios maliciosos;
R.HS205	Suportar o bloqueio automático de domínios maliciosos identificados com análise em tempo real;
R.HS206	Suportar a detecção de controle ou o roubo de dados usando tunelamento de DNS;
R.HS207	Suportar respostas dinâmicas automatizadas para encontrar máquinas infectadas;
R.HS208	Implementar e identificar existência de *malware* em anexos de e-mail e URL's conhecidas;
R.HS209	A solução deve possuir *engine* que seja possível não analisar determinada origem e/ou destino, configurados pelo administrador;
R.HS210	Identificar e bloquear a existência de *malware* em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;
R.HS211	Possuir mecanismo de bloqueio de vazamento, em tempo real, não intencional de dados originados de máquinas existentes no ambiente LAN de acordo com a classificação interna do arquivo;
R.HS212	Possuir funcionalidade de detecção e bloqueio imediato de *malwares* que utilizem mecanismo de exploração em arquivos no formado PDF;
R.HS213	A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais e aplicativos;
R.HS214	A tecnologia de máquina virtual em ambiente local ou de nuvem deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do *malware* ou código malicioso sem utilização de assinaturas;
R.HS215	Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema.
R.HS216	As atualizações deverão ser fornecidas pelo fabricante;
R.HS217	A solução deve possuir nuvem de inteligência proprietária do fabricante que seja responsável por atualizar toda a base de segurança através de assinaturas;

R.HS218	Implementar mecanismo de integração com servidores *syslog*;
R.HS219	A solução deve suportar as topologias de implantação *Inline* e *Mirror*/TAP;
R.HS220	A solução deve apresentar informações comportamentais, incluindo listagem de módulos e processos utilizados por *malware* e/ou código malicioso de forma sequencial;
R.HS221	Toda a análise e bloqueio de *malwares* e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato. Não serão aceitas soluções que apenas detectam o *malware* e/ou códigos maliciosos;
R.HS222	Implantar mecanismo do tipo de múltiplas fases para verificação de *malware* e/ou códigos maliciosos;
R.HS223	Deve possuir mecanismo de exceção, permitindo criação de regras por VLAN, subrede, endereço IP, grupo de usuários, domínio de destino, entre outros;
R.HS224	Implementar através da interface gráfica mecanismo de atualização da base de dados, sistema operacional e de *firmware* da solução;
R.HS225	A solução deve emular e eliminar *malwares* conhecidos em anexos de e-mail e documentos baixados na *web*;
R.HS226	A solução deve suportar a detecção e prevenção de vírus *cryptors* & *ransomware* e seus variantes, utilizando análises estáticas e dinâmicas;
R.HS227	O sistema de análise local deve prover informações sobre as ações da ameaça na máquina infectada, informações sobre quais aplicações são usadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *malware*, gerar assinaturas de contenção automaticamente, definir URL's não confiáveis utilizadas pelo novo *malware* e prover informações sobre o usuário infectado;
R.HS228	O sistema automático de análise local ou na nuvem deve emitir relatório com identificação do *malware*;
R.HS229	O sistema de emulação deve exibir a quantidade de arquivos analisados ou permitir a visualização de todos os arquivos analisados;
R.HS230	A solução deve possuir capacidade de executar arquivos em um ambiente simulado e controlado, local ou em nuvem;
R.HS231	Permitir o envio de arquivos para análise ambiente controlado de forma automática;
R.HS232	Suportar a análise de tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
R.HS233	Caso sejam necessárias licenças de sistema operacional e *softwares* para execução de arquivos no ambiente controlado, essas deverão ser fornecidas em sua totalidade sem custos adicionais;
R.HS234	A solução deverá possuir os indicadores referentes ao último dia, última semana ou últimos 30 dias para arquivos inspecionados e arquivos maliciosos encontrados;
R.HS235	Deve permitir exportar o resultado das análises de *malwares* de *zero-day* em PDF ou CSV, a partir da própria interface de gerência;
	FILTRO DE URL
R.HS236	Para prover maior visibilidade e controle dos acessos dos usuários do ambiente a solução deve incluir módulo de filtro de URL integrado;
R.HS237	Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
R.HS238	Deve ser possível criar políticas por usuários, grupo de usuários, IP's, redes e grupos de redes;

R.HS239	O mecanismo de controle de aplicação *web/url* deve apresentar contagem de utilização da regra;
R.HS240	A solução de Filtro de URL deverá ser totalmente integrada às Aplicações *Web* 2.0;
R.HS241	Deve possibilitar a inspeção de tráfego HTTPS;
R.HS242	A solução deve suportar a criação de mais de 600 regras de controle URL no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso;
R.HS243	A solução deve possuir *engine* de bloqueio de busca como *Google, Bing* e *Yahoo* independentemente se a opção *Safe Search* está habilitada no navegador do usuário;
R.HS244	Deverá permitir o controle, sem instalação de cliente de *software*, em equipamentos não autenticados, através de *Captive Portal*;
R.HS245	Equipamentos e usuários autenticados pelo *Active Directory* devem ser classificados de forma transparente de acordo com as políticas configuradas;
R.HS246	Deverá possuir suporte a identificação de usuários em *Microsoft Terminal Server*, permitindo visibilidade e controle sobre o uso das URL's que estão sendo acessadas através destes serviços;
R.HS247	A solução deve fornecer mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
R.HS248	Deverá incluir capacidade de configuração de políticas baseadas na visibilidade e controle de quem está usando tais URL's, através da integração com serviços de diretório, autenticação LDAP, *Active Directory* e base de dados local;
R.HS249	Suportar a criação de políticas baseadas no controle por URL e categoria de URL;
R.HS250	A solução deve ter uma base de URL que exceda 40 (quarenta) milhões de URL's categorizadas na base de dados do fabricante;
R.HS251	Suportar armazenamento de URL na própria solução evitando *delay* de comunicação/validação de URL's;
R.HS252	Suportar a criação de categorias de URL's customizadas;
R.HS253	Suportar a exclusão de URL's do bloqueio por categoria;
R.HS254	Permitir a customização da página de bloqueio que será mostrada para o usuário;
	IDENTIFICAÇÃO DE USUÁRIOS DA SOLUÇÃO
R.HS255	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando as aplicações e URL's através da integração com serviços de diretório, autenticação via LDAP, *Microsoft Active Directory*, RADIUS e base de dados local;
R.HS256	Deve possuir integração com *Microsoft Active Directory*, em diversos domínios simultaneamente para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupo de usuários sem a necessidade de instalar nenhum agente nos servidores *Active Directory* ou em máquina da rede;
R.HS257	Deve suportar o recebimento de eventos de autenticação de controlador wireless, dispositivo 802.1x, RADIUS ou *syslog*, para correlacionar endereços IP e usuários;
R.HS258	Para usuários não registrados ou não reconhecidos no domínio a solução deve ser capaz de fornecer uma autenticação baseada em navegador (*Captive Portal*), sem a necessidade de agente;
R.HS259	Deve possuir também suporte a autenticação via *Kerberos*;

R.HS260	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em *Microsoft Terminal Server*, permitindo visibilidade e controle granular;
R.HS261	A solução deverá ser capaz de identificar nome do usuário, *login* e IP registrados no *Microsoft Active Directory* de forma transparente para o usuário sem a necessidade de uso de agentes;
R.HS262	A solução deve suportar a opção de instalação de agentes em estações que possuam múltiplos usuários conectados simultaneamente com a finalidade de diferenciar os diferentes perfis em uso;
R.HS263	A solução deverá compartilhar e propagar a identificação de usuários com outros *gateways* de segurança do mesmo *cluster*;
R.HS264	Na integração com o *Active Directory*, todos os controladores de domínio em operação devem ser cadastrados sem a utilização de *scripts* de comando;
R.HS265	A solução de identificação de usuário deverá se integrar com as funcionalidades de *firewall*, controle de aplicação *web*, URL e Proteção contra Ameaças, sendo todas elas do mesmo fabricante e na mesma console de gerência;
	CARACTERÍSTICAS DE QOS
R.HS266	Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário;
R.HS267	Suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e *WhatsApp*);
R.HS268	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário;
	CARACTERÍSTICAS DE VPN
R.HS269	Deve disponibilizar licenciamento para VPN *site-to-site* e *client-to-site*, de forma a atender os itens abaixo;
R.HS270	Suportar, no mínimo, 1.000 (um mil) túneis VPN IPSec simultâneos;
R.HS271	Suportar, no mínimo, 5.000 (cinco mil) usuários VPN SSL;
R.HS272	Suportar VPN *site-to-site* em topologia *Full Meshed* (todos os *gateways* possuem *links* específicos para todos os demais *gateways*);
R.HS273	Suportar criptografia AES-128, AES-256;
R.HS274	Suportar integridade de dados com SHA-1 e SHA-256;
R.HS275	Suportar o protocolo IKE, fases I e II;
R.HS276	Suportar os algoritmos RSA e *Diffie-Hellman groups* 1, 2, 5 e 14;
R.HS277	Suportar NAT-T (NAT *Transversal*);
R.HS278	Suportar VPN IPSec *client-to-site*;
R.HS279	Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional e sem limite do número de usuários;
R.HS280	O cliente de VPN *client-to-site* deve ser compatível ou suportar o cliente nativo de pelo menos: Windows 10 (32 e 64 Bits), Apple IOS, Android, Mac OSx 10 ou Linux. Pode fornecer também, mas não obrigatória opção *Clientless* com autenticação via *browser*, para fechar a VPN através de um portal SSL;
R.HS281	Suportar atribuição de endereço IP nos clientes remotos de VPN;
R.HS282	Suportar atribuição de DNS nos clientes remotos de VPN;
R.HS283	Suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF ou BGP;

R.HS284	O túnel VPN do cliente ao *gateway* (*client-to-site*) deve fornecer uma solução de autenticação única (*sigle-sign-on*) aos usuários, integrando-se com as ferramentas de *Windows login*;
R.HS285	Deve permitir criar políticas por usuários e grupos para tráfego de VPN *client-to-site*;
R.HS286	Suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado ou CA externa de terceiros;
R.HS287	Deve promover a integração com diretórios *Active Directory* para a autenticação de usuários de VPN e regras de acesso;
R.HS288	Suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha do *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado ou CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
R.HS289	Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKLCS#12;
R.HS290	Suportar a solicitação de emissão de certificados a uma autoridade certificadora de confiança (*enrollment*) via SCEP (*Simple Certificate Enrollment Protocol*) ou CSR (*Certificate Signing Requests*);
R.HS291	Suportar a leitura e verificação de CRLs (*certification revogation lists*);
R.HS292	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

Requisitos Tecnológicos (hardware e software)	
ID	**Descrição**
R.HS293	Para efeitos deste Estudo Técnico, o uso das conjunções "e/ou" deve ser compreendido de forma ampla, ou seja, deve ser considerada a possibilidade de os elementos serem tomados em conjunto e, também, separadamente. Por exemplo, a expressão "Controle de políticas por porta e/ou protocolo" deve ser compreendida da seguinte forma: "O parâmetro para aplicação de políticas deve ser aplicado: a) por porta individualmente; b) por protocolo individualmente; e c) por porta e protocolo simultaneamente";
R.HS294	Cada solução de alta disponibilidade deverá ser composta por 2 (dois) equipamentos (*appliances*) funcionando em *cluster*, construídos especificamente para exercer a função de *Next Generation Firewall*, com *hardware* e *software* fornecidos pelo mesmo fabricante.
R.HS295	Deverá ser fornecida com licença(s) do(s) *software*(*s*) embutido(s) em todos os seus componentes, ou seja, durante a vigência do contrato, todas as atualizações deverão ser disponibilizadas ao Contratante. Após o seu término, a Contratante poderá continuar a utilizar o *firewall*, sem as funcionalidades de NGFW;
R.HS296	Deverá ser licenciado e habilitado para uso ilimitado de usuários e endereços IP;
R.HS297	Deverá possuir ao menos as seguintes funcionalidades nativas, que deverão operar na mesma solução: • *Firewall*; • Controle de Aplicação; • Gerenciamento de Qualidade de Serviço (QoS); • Prevenção contra Ameaças (IPS, *BotNets*); • Proteção contra Ameaças Avançadas; • Identificação de Usuários; • Filtro de URL; • Rede VPN; • Console de Gerenciamento e Monitoramento;
R.HS298	A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
R.HS299	Será aceita somente solução com as funcionalidades nativas descritas no item R.HS5 instaladas em ambiente físico local (*on-premise*), sendo vedada qualquer transmissão de informação para processamento na nuvem, exceto para atualização da base de dados da solução e prevenção contra ameaças avançadas;
R.HS299.1	Com relação à Proteção contra Ameaças Avançadas, poderá ser entregue equipamento físico exclusivo para essa finalidade com processamento local dos arquivos ou, caso a solução seja baseada em tratamento de dados na nuvem, essa deverá ser capaz de processar os arquivos definidos pela Contratante, independente do volume mensal, e agregar a proteção do tipo "*zero day*" par quaisquer situações;
R.HS300	Deve executar funcionalidades de proteção de rede, proteção e prevenção contra ameaças avançadas e não conhecidas, e somente será aceita solução (*hardware* e *software*) de um mesmo fabricante;

R.HS301	O *software* deverá ser fornecido em sua versão mais atualizada, relativo à data de sua instalação e configuração, não sendo permitido qualquer tipo de comprovação futura;
R.HS302	O *hardware* deve ser baseado em arquitetura que garanta flexibilidade e adaptação a novas ameaças sem impacto no desempenho;
R.HS303	A comunicação entre a solução de gerência e a solução de *hardware* de segurança, deverá ser criptografada;
R.HS304	Deve ser possível suportar arquitetura de armazenamento de *logs* redundante, permitindo a configuração de equipamentos distintos;
R.HS305	Possuir mecanismo de indexação de *logs* para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de *logs* mais antigos;
R.HS306	Os *gateways* de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;
R.HS307	Oferecer a funcionalidade de *backup*, assim como permitir ao administrador agendar procedimentos de *backups* periódicos;
	HARDWARE
R.HS308	Armazenamento de no mínimo de 1TB com 2 (dois) discos em RAID1, por equipamento, pois a falha do disco, se único, ocasionará indisponibilidade da solução bem como os dados de *log* nele existentes; • Caso a solução ofertada possua recurso de replicação síncrona de todos os dados para a solução de gerência, está será aceita.
R.HS309	Memória suficiente ou outra arquitetura que garanta desempenho sempre inferior a 75% de utilização da solução durante toda a vigência contratual; • O monitoramento poderá ser realizado tanto pelo sistema de gerenciamento centralizado ou por ferramenta própria de monitoração do TST, com intervalos mínimos de 5 minutos entre cada aferição.
R.HS310	Todos os equipamentos e seus componentes deverão ser novos, sem uso, entregues em perfeito funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.
R.HS311	Não serão aceitos equipamentos em modo *End of Life, End of Sale* e *End of Support*.
R.HS312	Mínimo de 4 (quatro) interfaces do tipo 10/100/1000 base-T RJ45 ou superior, com os respectivos *tranceivers*, para cada equipamento do *cluster*;
R.HS313	Mínimo de 4 (quatro) interfaces de rede do tipo 10Gbps SFP+, com os respectivos *tranceivers* bidirecional, com conector LC, para cada equipamento do *cluster*;
R.HS314	Mínimo de 4 (quatro) interfaces tipo 40Gbps QSFP+ bidirecional, com os respectivos *tranceivers* com conector LC, para cada equipamento do *cluster*;
R.HS315	Mínimo de 1 (uma) interface, dedicada para gerenciamento;
R.HS316	Mínimo de 1 (uma) interface, dedicada para console;
R.HS317	Mínimo de 1 (uma) interface, dedicada para sincronismo do *cluster*;
R.HS318	Mínimo de 1 (uma) interface, dedicada para gerenciamento *out-of-band*;
R.HS319	Fonte de alimentação 120/240 VAC, redundante e *hot-swappable*;
R.HS320	Ser apropriado para o uso em ambiente tropical com umidade relativa na faixa de 10 a 99% (sem condensação) e temperatura ambiente na faixa de 0°C a 40°C.
R.HS321	Vir acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos, etc.) para fixação em bastidor (*rack*) padrão EIA-310 com largura de 19"(dezenove polegadas).

R.HS322	Possuir certificação de conformidade sustentável de acordo com os padrões EPA (*Enviromental Protection Agency*) ou similar, tais como, *EnergyStar*, *RoHS* (*Restriction on Harzadous Substances*), WEEE (*Waste Electrical and Eletronic Equipament*) ou EMI *Certifications* FCC *part* 15, CE, EN55022, EN55024.
R.HS323	Possuir *throughput* de proteção de, no mínimo, 15 (quinze) Gbps para as funcionalidades de *firewall*, Controle de Aplicação, Prevenção de Ameaças (IPS, *BotNets* e Antivírus), Proteção contra Ameaças Avançadas, Filtro de URL, Identificação de Usuários da Solução, Características de *QoS*, características de VPN habilitadas simultaneamente;
R.HS323.1	O *throughput* é considerado como a quantidade de tráfego que um único equipamento consegue redirecionar. Caso a fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será considerado.
R.HS324	Suportar, no mínimo, 8.000.000 (oito milhões) de conexões concorrentes;
R.HS325	Suportar, no mínimo, 200.000 (duzentos mil) novas conexões por segundo;
R.HS326	As taxas de transferência indicadas devem ser alcançadas com a inspeção integral de todos os pacotes de dados, independentemente de seu tamanho ou direção de fluxo, sem prejuízo no desempenho do equipamento, e com todas as assinaturas, lista e demais métodos de controle de acesso e de detecção e prevenção de ameaças habilitados;

	FIREWALL
R.HS327	Suportar os protocolos IPv4 e IPv6;
R.HS328	Suportar no mínimo 1024 VLANs no padrão 802.1q e estabelecer regras de filtragem (*Stateful Firewall*) entre elas;
R.HS329	Suportar agregação de *links* no padrão 802.3ad;
R.HS330	Suportar *policy based routing* ou *policy based forwarding*, possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;
R.HS331	Suportar roteamento *multicast* (PIM-SM);
R.HS332	Suportar DHCP *Relay* e DHCP *Server*;
R.HS333	Suportar *jumbo frames*;
R.HS334	Suportar NAT dinâmico (N-to-1 e N-to-N);
R.HS335	Suportar NAT estático (N-to-1 e N-to-N);
R.HS336	Suportar NAT estático bidirecional (1-to-1);
R.HS337	Suportar tradução de porta (PAT);
R.HS338	Suportar NAT de origem e NAT de destino, simultaneamente;
R.HS339	Enviar *log* para sistemas de monitoramento externos, simultaneamente aos registros internos;
R.HS340	Deve implementar mecanismo de proteção contra ataques de falsificação de endereços IP (*anti-spoofing*) para IPv4;
R.HS341	Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
R.HS342	Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
R.HS343	Suportar OSPF *graceful restart*;
R.HS344	Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente e em *layer* 3;
R.HS345	Os dispositivos de proteção devem ter a capacidade de operar de forma simultânea mediante o uso de suas interfaces físicas nos seguintes modos: • Modo *sniffer* (monitoramento e análise do tráfego de rede), camada 2 e camada 3; • Modo *sniffer*, para inspeção via porta espelhada do tráfego de dados da rede; • Modo Camada 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação; • Modo Camada 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como *default gateway* das redes protegidas; • Modo Misto de trabalho *sniffer*, L2 e L3, em diferentes interfaces físicas.
R.HS346	A configuração em alta disponibilidade deverá ser implantada de forma a suportar *clusters* ativo/ativo e ativo*/standby*, devendo sincronizar: • Sessões; • Configurações, incluindo, mas não limitado a políticas de *firewall*; • NAT, QoS e objetos de rede; • Associação de Segurança das VPNs; • Tabelas FIB; • Tabelas de usuários autenticados.
R.HS347	O HA deve possibilitar monitoramento de falha de *link*;
R.HS348	Suportar atuação como cliente NTP (*network time protocol*);

	CONTROLE POR POLÍTICAS DE SEGURANÇA
R.HS349	A solução de segurança deve usar *Stateful Inspection* baseada na análise de comunicação e de estado da conexão para monitorar e controlar o fluxo de rede;
R.HS350	Permitir a implementação de monitoramento de *links* de Internet, através de teste de conectividade com endereços específicos, e implantar alertas em caso de quedas;
R.HS351	As regras deverão ser elaboradas utilizando objetos de rede baseados em TCP/IP. Durante a criação da regra, tais objetos deverão ser associados sem que haja necessidade de associação à interface de rede de origem ou destino da conexão ou então permitir a configuração para todas as interfaces simultaneamente;
R.HS352	Possibilitar a configuração, entre os nós do *cluster*, no mínimo, nos modos Ativo/Ativo e Ativo/*Standby*, garantindo assim, que apenas um dos nós consiga suportar toda a demanda dessa especificação técnica;
R.HS353	Após uma queda ou reconexão de qualquer dos *links*, deve ser possível configurar ações como alertas SNMP, armazenamento do *log* *scripts* customizados pelo usuário;
R.HS354	Autenticar sessões ou usuários para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;
R.HS355	Controles de políticas por porta e/ou protocolo;
R.HS356	Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;
R.HS357	A base de categorias e aplicações deve ser fornecida e constantemente atualizada pelo fabricante da solução, sempre que uma alteração em sua base seja feita. Deve permitir, ainda, que algum objeto seja sobrescrito por configuração do próprio administrador;
R.HS358	Controle de políticas por usuários, grupos de usuários, IPs, redes e/ou grupos de redes;
R.HS359	Controle de políticas por código de Países, sem que seja necessário configurar manualmente o escopo de endereço desses países;
R.HS360	Suportar a criação de políticas por geolocalização, permitindo que o tráfego de entrada e/ou de saída de determinado(s) país(es) seja(m) bloqueado(s);
R.HS361	Deve decriptografar tráfego *inbound* e *outbound* em conexões negociadas com, no mínimo, TLS 1.1 e TLS 1.2;
R.HS362	Bloqueio dos seguintes tipos de arquivos como *bat, cab, dll, exe, pif* e *reg* e outros, de acordo com a necessidade, configuráveis através do *software* de gerência disponibilizado;
R.HS363	*Traffic shapping* e *QoS* – priorização de tráfego de dados baseada em Políticas (Prioridade, Garantia e Limitação máxima);
R.HS364	*QoS* (qualidade de serviço) baseada em políticas para marcação de pacotes (*diffserv marking*);
R.HS365	Suporte a configuração de regras que permitam informar endereço IP nas versões IPv4 e IPv6, sem duplicação de regra;
R.HS366	Suporte a objetos e regras *multicast*;
R.HS367	Permitir o agendamento de aplicação automática de políticas em horário pré-definidos pelos administradores;
R.HS368	Deve suportar importação de certificado em inspeção de conexões SSL de entrada (*inbound*);

R.HS369	A solução deve ser capaz de identificar o comportamento do protocolo SSH, onde pode ser feito através de padrões de análise de protocolo;
R.HS370	Deve ter a capacidade de inspecionar e bloquear tráfego operando em camada 2 e camada 3;
R.HS371	Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações;
R.HS372	Deve inspecionar e bloquear os dados operando como *default gateway* das redes protegidas e controlar o tráfego em nível de aplicações;
R.HS373	Na ocorrência de falhas, as conexões existentes em um *firewall* deverão ser mantidas pelo(s) outro(s), sem perdas destas conexões, não acarretando interrupções no tráfego da rede e nem redução de desempenho da solução;
R.HS374	Na aplicação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas;
R.HS375	Promover a integração com diretório LDAP (X.500) e *Active Directory* para a autenticação de usuários, de modo que o *Firewall* possa utilizar das informações armazenadas para realizar autenticações;
R.HS376	Para configuração a administração do *Firewall* deve possibilitar o acesso via CLI (SSH), console do fabricante e interface *web* HTTPS;
R.HS377	A solução de *Firewall* deve prover funcionalidade que permita visualização do grau de utilização de cada regra, por exemplo, quantidade de *hits* por regra, % de utilização ou volume em *bytes*;
R.HS378	A solução deve, por padrão, não permitir que ataque do tipo "*scan ports*" ou similares retornem resultados do estado das portas;
R.HS379	A solução de *Firewall* deve suportar no mínimo, 10.000 (dez mil) regras;
R.HS380	A solução deve suportar o mínimo de 16.384 entradas de endereço ARP;
R.HS381	Deverá permitir a aceleração e otimização da leitura das regras, de modo que o *firewall* consiga identificar padrões muito utilizados;
R.HS382	Deverá suportar métodos de autenticação de, no mínimo, usuário e cliente;
R.HS383	A solução deverá disponibilizar interface para gerenciamento das atualizações de segurança para instalação agendada ou automática, conforme determinação da Contratante;
	CONTROLE DE APLICAÇÕES
R.HS384	A solução deverá contar com ferramentas de visibilidade e controle de aplicações *web* integradas na própria solução de segurança, que permitam a criação de políticas de liberação ou bloqueio baseando-se em aplicações *web* 2.0;
R.HS385	Deve prover o controle e a proteção de acesso à Internet por meio do reconhecimento das aplicações *web 2.0*, independente de porta e protocolo, e da classificação de URL's;
R.HS386	Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;
R.HS387	Deve ser capaz de identificar um mínimo de 2.000 (duas mil) aplicações, incluindo, mas não se limitando a: *peer-to-peer*, *streaming* de áudio e vídeo, *update* de *software*, *instant messaging*, redes sociais, *proxies*, *anonymizers*, acesso e controle remoto, VoIP e e-mail;
R.HS388	Deve ser capaz de identificar, no mínimo, as seguintes aplicações: *BitTorrent*, *Youtube*, *Livestream*, *Skype*, *Viber*, *WhatsApp*, *Snapchat*, *Facebook*, *Facebook Messenger* ou *Facebook Chat*, *G Suite*, *Tinder*, *Instagram*, *Twitter*, *Linkedin*, *Dropbox*, *One* Drive ou *Microsoft One Drive*, *Logmein*, *TeamViewer*, MS-RDP, VNC, *Ultrasurf*, TOR, *Webex*, *Evernot*, *Amazon Cloud Drive*, *Gotomeeting*.

R.HS389	Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, *social widgets* (ou similar) com controle granular para usuários ou grupos de usuários;
R.HS390	A solução deverá possuir pelo menos as categorias de aplicações *web* pré-definidas pelo fabricante, atualizadas em tempo real;
R.HS391	Deve possibilitar a inspeção de tráfego HTTPS (*inbound/outbound*);
R.HS392	Deve ser capaz de identificar aplicações criptografadas usando SSL;
R.HS393	Deve possibilitar o bloqueio das aplicações, de portas e protocolos;
R.HS394	Deve possibilitar a criação de regras com várias categorias;
R.HS395	Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reiniciar os *gateways* e gerência;
R.HS396	Deve possibilitar a permissão ou bloqueio de aplicações por, pelo menos, os seguintes critérios: • Aplicação da *web*; • Categorias; • IP/Range de IP's/Redes; • Usuários do AD/LDAP; • Grupos de usuários do AD/LDAP; • Aplicações tais como *Ultrasurf*, *Torrent*, *Dropbox* e demais *File Sharing.*
R.HS397	Deve possibilitar a customização da tela de interação com o usuário, permitindo: • Informar sobre o bloqueio; • Questionar sobre a necessidade de acesso. •
R.HS398	Deve possibilitar a customização de regra utilizando as seguintes ações de controle: • Permitir; • Bloquear; • Bloquear e informar; • Monitorar; • Informar o usuário.
R.HS399	Deve permitir o bloqueio total de aplicações do tipo *proxy* (*Ultrasurf, Tor, etc.*);
R.HS400	Deve possibilitar a integração da solução com base do *Microsoft Active Directory*, LDAP, RADIUS ou base local para criação de políticas utilizando: • Usuários; • Grupo de Usuários; • Objetos cadastrados vinculados ao endereço IP; • Endereço IP; • Endereço de Rede; • Combinação das opções acima.
R.HS401	A solução deve suportar a criação de pelo menos 600 regras de controle de aplicações no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso;
R.HS402	O mecanismo de Controle de aplicação *Web*/URL deve apresentar contagem de utilização de regra de acordo com a utilização;
R.HS403	A solução deve ter um mecanismo configurável de *by-pass*, onde o administrador consegue definir grupos específicos de usuários ou de máquinas que estão autorizados a ignorar as regras de inspeção SSL;
R.HS404	Deverá categorizar as aplicações ou URL's por fator de risco;

R.HS405	A solução deverá receber atualizações, para sua base de aplicações e URL's, a partir de um serviço baseado em nuvem, fornecido pelo fabricante da solução;
R.HS406	A solução deverá possuir uma console gráfica centralizada para gerenciar regras de *firewall*, de aplicações e de URL's;
R.HS407	Deverá possuir um mecanismo para informar ou perguntar ao usuário, em tempo real, com a finalidade de educa-los ou confirmar ações baseadas na política de acesso;
R.HS408	Deverá permitir a criação de exceções baseadas em objetos de rede;
R.HS409	A solução deve prover a opção de editar a notificação de bloqueio e redirecionar o usuário para a página de remediação;
R.HS410	Deve incluir o mecanismo de *black list* e *white list* permitindo ao administrador do sistema negar ou permitir o acesso a determinadas URL's, independente da categoria;
R.HS411	Deve inspecionar o *payload* do pacote de dados com o objetivo de detectar, através de expressões regulares (ou similar), assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta *default* ou não, incluindo, mas não se limitando ao uso de protocolo *Remote Desktop Protocol* na porta 80 ao invés da porta 3389;
R.HS412	Para tráfego criptografado (SSL), deve decriptografar pacotes a fim de possibilitar a leitura do *payload* para checagem de assinaturas de aplicações conhecidas pelo fabricante;
R.HS413	Deve realizar a decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
R.HS414	A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação, incluindo, mas não se limitando a compartilhamento de arquivo de soluções;
R.HS415	Deve detectar arquivos e outros conteúdos que devem ser inspecionados de acordo com as regras de segurança implementadas em outras camadas;
R.HS416	Identificar o uso de técnicas evasivas através de comunicações criptografadas;
R.HS417	Limitar a banda (*download/upload*) usada por aplicações baseado no IP de origem, usuários e grupos do LDAP/AD;
R.HS418	Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário d rede em tempo real com integração ao *Microsoft Active Directory*, sem a necessidade de instalação de agente no *Domain Controller*, nem nas estações dos usuários;
R.HS419	Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
R.HS420	Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do TST;
R.HS421	O fabricante deve permitir a solicitação de inclusão ou alteração de categorização na base de assinaturas das aplicações;
R.HS422	Deve alertar o usuário quando uma aplicação for bloqueada;
R.HS423	Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
R.HS424	Deve possibilitar a diferenciação de tráfego de *Instant Messaging* possuindo granularidade de controle e/ou políticas;

R.HS425	Deve possibilitar a diferenciação e controle de partes das aplicações como, por exemplo, permitir o *Whatsapp* e bloquear a transferência de arquivos;
R.HS426	Deve permitir a criação de regras de liberação e bloqueio utilizando apenas o domínio, usando expressões regulares, sem necessidade de inserção do endereço IP pelo administrador, onde a resolução deve ser feita de forma automática e em tempo real pela solução, inclusive para consultas baseadas em nuvem.
R.HS427	Deve ser possível a criação de grupos estáticos e dinâmicos de aplicações;
	PREVENÇÃO DE AMEAÇAS
R.HS428	Deve incluir assinaturas de prevenção de intrusão, IPS, e suporte ao bloqueio de arquivos e códigos maliciosos;
R.HS429	Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar: *Antivírus*, *Antimalware* e *BotNets* integrados na própria solução de *firewall* sem a necessidade de uso de quaisquer interfaces externas, onde sua console de gerência deverá residir na mesma console centralizada;
R.HS430	Deve sincronizar as assinaturas de prevenção de ameaças por demanda ou por agendamento;
R.HS431	As assinaturas devem permitir a ativação e desativação, ou ainda, ativação apenas em modo de monitoramento;
R.HS432	Exceções por IP de origem ou destino devem ser possíveis, de forma geral e assinatura-a-assinatura;
R.HS433	Deve suportar granularidade nas políticas de *Antivírus* e *Antimalware*, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, grupo de usuários, serviço ou assinatura e a combinação de todos esses itens;
R.HS434	Deve suportar o bloqueio de vulnerabilidades;
R.HS435	Deve incluir proteção contra ataque de negação de serviços (*DoS* e *DDoS*);
R.HS436	Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos os seguintes ataques conhecidos: SQL *Injection*, ICMP *denial of servisse*, força bruta e *port scanner*, SMB, *Port overflow*, *Non compliant* SSL;
R.HS437	Deverá possuir mecanismos de detecção de assinaturas, anomalias de protocolos, controle de aplicações e detecção de comportamento;
R.HS438	A solução de IPS deve fazer a inspeção de toda a sessão, independentemente do tamanho, de forma bidirecional, sem degradas o desempenho do equipamento;
R.HS439	O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar a solução;
R.HS440	Deve estar incluso informações como código CVE (*Common Vulnerabilities and Exposures*), severidade e tipo de ação a ser executada em cada proteção de segurança, mesmo que de forma manual;
R.HS441	Deve ser capaz de bloquear tráfego SSH enviado em portas diferentes da porta padrão;
R.HS442	As regras de exceção deverão possuir origem, destino, serviço, severidade, grupo de usuário ou alguma dessas combinações;
R.HS443	A solução deve ser capaz de inspecionar tráfego HTTPS de entrada e saída;
R.HS444	A solução de IPS integrada na solução de segurança deve possuir uma base de assinatura não inferior a 10.000 (dez mil) assinaturas;

R.HS445	A solução de IPS deve possuir funcionalidade que permita configurar as assinaturas do IPS o modo apenas de detecção para fins de *troubleshooting*;
R.HS446	A solução de IPS deve possuir índices por período que apontem o nível de ação das assinaturas baseado pela sua severidade na própria interface de gerência;
R.HS447	A solução deve permitir incorporar de forma automática novas proteções de IPS através de sua severidade;
R.HS448	O módulo de IPS deve possuir assinaturas voltadas para ambiente de servidores *web* e DNS;
R.HS449	A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação protegendo, pelo menos, os seguintes serviços: Aplicações *web*, serviços de e-mail, DNS, FTP, serviços *Windows* (*Microsoft Networking*) e VoIP;
R.HS450	A solução deve permitir ao administrador configurar quais métodos e comandos HTTP e comandos FTP são permitidos e quais são bloqueados;
R.HS451	Deve incluir proteção contra vírus e *worms* em conteúdo *ActiveX*, *applets Java* e outros;
R.HS452	Deve possuir perfis pré-configurados de proteção de IPS que podem ser utilizados a qualquer momento;
R.HS453	Deve incluir tela de visualização a fim de monitorar graficamente a quantidade de alertas de diferentes severidades. As diferentes áreas de interesse devem ser definidas utilizando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades da solução, incluindo pelo menos: origem, destino, serviço, usuário, tipo e nome do alerta;
R.HS454	A solução deve permitir a configuração de inspeção do IPS baseada em políticas que utilizem o posicionamento geográfico de origens ou destinos e combinações entre os dois;
R.HS455	A solução de possuir esquemas de atualização de assinaturas, no mínimo, através de agendamento, modo *off-line* e por demanda;
R.HS456	A solução deverá possuir relatório e correlação de eventos centralizada;
R.HS457	A solução deverá permitir a ativação de novas proteções baseada em parâmetros configuráveis como: severidade da ameaça, proteções para clientes e proteções para servidores;
R.HS458	A solução deve proteger contra ataques do tipo DNS *Cache Poisoning* e impedir que os usuários acessem endereços de domínios bloqueados;
R.HS459	A solução deve permitir bloquear o tráfego de entrada e/ou saída com base em países, sem a necessidade de gerir manualmente o *range* de endereços IP dos países que se deseja bloquear;
R.HS460	Ser imune e capaz de impedir ataques básicos como: SYN *flood*, ICMP *flood*, UDP *flood*;
R.HS461	Suportar análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;
R.HS462	A solução deverá realizar análise de *malware,* em sistemas físicos exclusivos (*bare metal*), evitando a atuação de *malwares* que reconheçam sistemas de *sandbox*;
R.HS463	Deverá ser capaz de decriptografar para análise pelo menos os protocolos SSL, SSH e SCP;
R.HS464	Deverá ser capaz de implementar autenticação para aplicações de multifator (MFA) ;
R.HS465	Detectar e bloquear a origem de *port scans*;
R.HS466	Possuir assinaturas para bloqueio de ataques de *buffer overflow*;

R.HS467	Suportar o bloqueio de vírus e *spywares*;
R.HS468	Suportar bloqueio de arquivos por tipo ou extensão;
R.HS469	Identificar e bloquear comunicação com *BotNets*;
R.HS470	Deve suportar referência cruzada com CVE (*Common Vulnerabilities and Exposures*);
R.HS471	A solução deve possuir nuvem de inteligência proprietária do fabricante, que seja responsável em atualizar toda a base de segurança do *appliances* através de assinaturas, durante a vigência do contrato;
R.HS472	Implementar modo de configuração totalmente transparente para o usuário final de modo que não haja necessidade de configuração de *proxies*, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;
R.HS473	Implementar funcionalidade de detecção e bloqueio de *call-backs* (comunicação do *malware* com o servidor de comando e controle);
R.HS474	A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede, baseado em análises de tráfego de rede, processamento de pacotes, dentre outros;
R.HS475	A solução de proteção contra *BotNets* deve utilizar mecanismo de detecção em multicamadas, que inclui reputação ode endereço IP, URLs e endereços DNS, assim como detecção de padrões de comunicação BOT;
R.HS476	O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regras individuais visando aperfeiçoar o desempenho do equipamento;
R.HS477	A solução de segurança deve permitir o bloqueio de *download* de arquivos que exceda tamanho pré-definido;
R.HS478	A solução deve analisar e bloquear *malwares* e/ou códigos maliciosos pelo menos nos seguintes tipos de arquivos do pacote *office* (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), MacOS (*mach*-O, DMG e PKG), *Linux* (ELF), RAR e 7-ZIP, análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL;
R.HS479	A solução deve realizar a análise dos arquivos de *download* anteriormente a entrega ao usuário;
R.HS480	Possuir antivírus em tempo real para ambiente de *gateway* internet, integrado à plataforma de proteção para os protocolos HTTP, HTTPS e SMTP;
R.HS481	A solução deve atuar na prevenção de forma granular através de políticas por usuário/máquina ou rede, sendo possível escolher um perfil diferente para cada regra ou prover todas as informações necessárias no *log* para a criação da exceção de forma manual;
R.HS482	A solução deve permitir criar regras de exceção de acordo com a proteção a partir do *log* visualizado na interface gráfica da gerência centralizada;
R.HS483	A solução de relatório deve apresentar via interface gráfica, no mínimo, informações de *hosts* infectados, atividades de *malware* e detalhes dos alertas;
R.HS484	Deve possuir visualização na própria interface de gerência dos maiores incidentes através de *hosts* ou incidentes de vírus e *bots*;
R.HS485	A solução deve permitir compartilhar informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do fabricante;
R.HS486	Permitir o bloqueio de *malwares*;
R.HS487	A solução deverá ser capaz de manter a análise de antivírus em caso de falha de conexão com a nuvem, bem como permitir criação de regras exceção para análise de antivírus;
R.HS488	A solução deverá possuir mecanismo para proteger contra ataques de *phishing*;

R.HS489	A solução deve ser capaz de proteger contra ataques DNS, tais como capacidade de detectar e prevenir C&C DNS *Hide Out*, analisar padrões de comunicação C&C e não apenas o servidor DNS de destino, realizar engenharia reversa do *malware*, detecção passiva de DNS e de comando e controle (C&C) e capacidade para detectar e prevenir ataques DNS *tunneling*;
R.HS490	A solução deverá suportar análise de arquivos que trafegam dentro do protocolo SMB, versões 2 e 3;
R.HS491	Deve suportar a inspeção em arquivos compactados;
	PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS
R.HS492	A solução deverá prover as funcionalidades de inspeção de tráfego de entrada de *malwares* não conhecidos (APT *Advanced Persistent Threat* e *Zero-Day Threats*), *ransomwares* com filtro de ameaças avançadas e análise de execução em tempo real e inspeção de tráfego de saída de *call-backs*;
R.HS493	Possuir capacidade de prevenção de ameaças não conhecidas;
R.HS494	A solução deve possuir funcionalidades para prevenção de *malwares* não conhecidos, incluídas na própria ferramenta (*zero-day*);
R.HS495	Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS e SMTP;
R.HS496	Deve ser capaz de inspecionar tráfego criptografado usando SSL;
R.HS497	A solução deve possuir mecanismo para identificar *hosts* infectados tentando acessar endereços de DNS de domínios maliciosos;
R.HS498	Suportar o bloqueio automático de domínios maliciosos identificados com análise em tempo real;
R.HS499	Suportar a detecção de controle ou o roubo de dados usando tunelamento de DNS;
R.HS500	Suportar respostas dinâmicas automatizadas para encontrar máquinas infectadas;
R.HS501	Implementar e identificar existência de *malware* em anexos de e-mail e URL's conhecidas;
R.HS502	A solução deve possuir *engine* que seja possível não analisar determinada origem e/ou destino, configurados pelo administrador;
R.HS503	Identificar e bloquear a existência de *malware* em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;
R.HS504	Possuir mecanismo de bloqueio de vazamento, em tempo real, não intencional de dados originados de máquinas existentes no ambiente LAN de acordo com a classificação interna do arquivo;
R.HS505	Possuir funcionalidade de detecção e bloqueio imediato de *malwares* que utilizem mecanismo de exploração em arquivos no formado PDF;
R.HS506	A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais e aplicativos;
R.HS507	A tecnologia de máquina virtual em ambiente local ou de nuvem deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do *malware* ou código malicioso sem utilização de assinaturas;
R.HS508	Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema.
R.HS509	As atualizações deverão ser fornecidas pelo fabricante;
R.HS510	A solução deve possuir nuvem de inteligência proprietária do fabricante que seja responsável por atualizar toda a base de segurança através de assinaturas;

R.HS511	Implementar mecanismo de integração com servidores *syslog*;
R.HS512	A solução deve suportar as topologias de implantação *Inline* e *Mirror*/TAP;
R.HS513	A solução deve apresentar informações comportamentais, incluindo listagem de módulos e processos utilizados por *malware* e/ou código malicioso de forma sequencial;
R.HS514	Toda a análise e bloqueio de *malwares* e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato. Não serão aceitas soluções que apenas detectam o *malware* e/ou códigos maliciosos;
R.HS515	Implantar mecanismo do tipo de múltiplas fases para verificação de *malware* e/ou códigos maliciosos;
R.HS516	Deve possuir mecanismo de exceção, permitindo criação de regras por VLAN, subrede, endereço IP, grupo de usuários, domínio de destino, entre outros;
R.HS517	Implementar através da interface gráfica mecanismo de atualização da base de dados, sistema operacional e de *firmware* da solução;
R.HS518	A solução deve emular e eliminar *malwares* conhecidos em anexos de e-mail e documentos baixados na *web*;
R.HS519	A solução deve suportar a detecção e prevenção de vírus *cryptors* & *ransomware* e seus variantes, utilizando análises estáticas e dinâmicas;
R.HS520	O sistema de análise local deve prover informações sobre as ações da ameaça na máquina infectada, informações sobre quais aplicações são usadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *malware*, gerar assinaturas de contenção automaticamente, definir URL's não confiáveis utilizadas pelo novo *malware* e prover informações sobre o usuário infectado;
R.HS521	O sistema automático de análise local ou na nuvem deve emitir relatório com identificação do *malware*;
R.HS522	O sistema de emulação deve exibir a quantidade de arquivos analisados ou permitir a visualização de todos os arquivos analisados;
R.HS523	A solução deve possuir capacidade de executar arquivos em um ambiente simulado e controlado, local ou em nuvem;
R.HS524	Permitir o envio de arquivos para análise ambiente controlado de forma automática;
R.HS525	Suportar a análise de tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
R.HS526	Caso sejam necessárias licenças de sistema operacional e *softwares* para execução de arquivos no ambiente controlado, essas deverão ser fornecidas em sua totalidade sem custos adicionais;
R.HS527	A solução deverá possuir os indicadores referentes ao último dia, última semana ou últimos 30 dias para arquivos inspecionados e arquivos maliciosos encontrados;
R.HS528	Deve permitir exportar o resultado das análises de *malwares* de *zero-day* em PDF ou CSV, a partir da própria interface de gerência;
	FILTRO DE URL
R.HS529	Para prover maior visibilidade e controle dos acessos dos usuários do ambiente a solução deve incluir módulo de filtro de URL integrado;
R.HS530	Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
R.HS531	Deve ser possível criar políticas por usuários, grupo de usuários, IP's, redes e grupos de redes;

R.HS532	O mecanismo de controle de aplicação *web/url* deve apresentar contagem de utilização da regra;
R.HS533	A solução de Filtro de URL deverá ser totalmente integrada às Aplicações *Web* 2.0;
R.HS534	Deve possibilitar a inspeção de tráfego HTTPS;
R.HS535	A solução deve suportar a criação de mais de 600 regras de controle URL no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso;
R.HS536	A solução deve possuir *engine* de bloqueio de busca como *Google, Bing* e *Yahoo* independentemente se a opção *Safe Search* está habilitada no navegador do usuário;
R.HS537	Deverá permitir o controle, sem instalação de cliente de *software*, em equipamentos não autenticados, através de *Captive Portal*;
R.HS538	Equipamentos e usuários autenticados pelo *Active Directory* devem ser classificados de forma transparente de acordo com as políticas configuradas;
R.HS539	Deverá possuir suporte a identificação de usuários em *Microsoft Terminal Server*, permitindo visibilidade e controle sobre o uso das URL's que estão sendo acessadas através destes serviços;
R.HS540	A solução deve fornecer mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;
R.HS541	Deverá incluir capacidade de configuração de políticas baseadas na visibilidade e controle de quem está usando tais URL's, através da integração com serviços de diretório, autenticação LDAP, *Active Directory* e base de dados local;
R.HS542	Suportar a criação de políticas baseadas no controle por URL e categoria de URL;
R.HS543	A solução deve ter uma base de URL que exceda 40 (quarenta) milhões de URL's categorizadas na base de dados do fabricante;
R.HS544	Suportar armazenamento de URL na própria solução evitando *delay* de comunicação/validação de URL's;
R.HS545	Suportar a criação de categorias de URL's customizadas;
R.HS546	Suportar a exclusão de URL's do bloqueio por categoria;
R.HS547	Permitir a customização da página de bloqueio que será mostrada para o usuário;
	IDENTIFICAÇÃO DE USUÁRIOS DA SOLUÇÃO
R.HS548	Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando as aplicações e URL's através da integração com serviços de diretório, autenticação via LDAP, *Microsoft Active Directory*, RADIUS e base de dados local;
R.HS549	Deve possuir integração com *Microsoft Active Directory*, em diversos domínios simultaneamente para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupo de usuários sem a necessidade de instalar nenhum agente nos servidores *Active Directory* ou em máquina da rede;
R.HS550	Deve suportar o recebimento de eventos de autenticação de controlador wireless, dispositivo 802.1x, RADIUS ou *syslog*, para correlacionar endereços IP e usuários;
R.HS551	Para usuários não registrados ou não reconhecidos no domínio a solução deve ser capaz de fornecer uma autenticação baseada em navegador (*Captive Portal*), sem a necessidade de agente;
R.HS552	Deve possuir também suporte a autenticação via *Kerberos*;

R.HS553	Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em *Microsoft Terminal Server*, permitindo visibilidade e controle granular;
R.HS554	A solução deverá ser capaz de identificar nome do usuário, *login* e IP registrados no *Microsoft Active Directory* de forma transparente para o usuário sem a necessidade de uso de agentes;
R.HS555	A solução deve suportar a opção de instalação de agentes em estações que possuam múltiplos usuários conectados simultaneamente com a finalidade de diferenciar os diferentes perfis em uso;
R.HS556	A solução deverá compartilhar e propagar a identificação de usuários com outros *gateways* de segurança do mesmo *cluster*;
R.HS557	Na integração com o *Active Directory*, todos os controladores de domínio em operação devem ser cadastrados sem a utilização de *scripts* de comando;
R.HS558	A solução de identificação de usuário deverá se integrar com as funcionalidades de *firewall*, controle de aplicação *web*, URL e Proteção contra Ameaças, sendo todas elas do mesmo fabricante e na mesma console de gerência;
	CARACTERÍSTICAS DE QOS
R.HS559	Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário;
R.HS560	Suportar a criação de políticas de controle de uso de largura de banda baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, Youtube e *WhatsApp*);
R.HS561	Suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP, SCCP e MGCP;
R.HS562	Suportar a marcação de pacotes *DiffServ*;
R.HS563	Deve permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário;
	CARACTERÍSTICAS DE VPN
R.HS564	Deve disponibilizar licenciamento para VPN *site-to-site* e *client-to-site*, de forma a atender os itens abaixo;
R.HS565	Suportar, no mínimo, 1.000 (um mil) túneis VPN IPSec simultâneos;
R.HS566	Suportar, no mínimo, 5.000 (cinco mil) usuários VPN SSL;
R.HS567	Suportar VPN *site-to-site* em topologia *Full Meshed* (todos os *gateways* possuem *links* específicos para todos os demais *gateways*);
R.HS568	Suportar criptografia AES-128, AES-256;
R.HS569	Suportar integridade de dados com SHA-1 e SHA-256;
R.HS570	Suportar o protocolo IKE, fases I e II;
R.HS571	Suportar os algoritmos RSA e *Diffie-Hellman groups* 1, 2, 5 e 14;
R.HS572	Suportar NAT-T (NAT *Transversal*);
R.HS573	Suportar VPN IPSec *client-to-site*;
R.HS574	Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional e sem limite do número de usuários;
R.HS575	O cliente de VPN *client-to-site* deve ser compatível ou suportar o cliente nativo de pelo menos: Windows 10 (32 e 64 Bits), Apple IOS, Android, Mac OSx 10 ou Linux. Pode fornecer também, mas não obrigatória opção *Clientless* com autenticação via *browser*, para fechar a VPN através de um portal SSL;
R.HS576	Suportar atribuição de endereço IP nos clientes remotos de VPN;
R.HS577	Suportar atribuição de DNS nos clientes remotos de VPN;

R.HS578	Suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF ou BGP;
R.HS579	O túnel VPN do cliente ao *gateway* (*client-to-site*) deve fornecer uma solução de autenticação única (*sigle-sign-on*) aos usuários, integrando-se com as ferramentas de *Windows login*;
R.HS580	Deve permitir criar políticas por usuários e grupos para tráfego de VPN *client-to-site*;
R.HS581	Suportar autoridade certificadora integrada ao gateway VPN ou à solução de gerenciamento centralizado ou CA externa de terceiros;
R.HS582	Deve promover a integração com diretórios *Active Directory* para a autenticação de usuários de VPN e regras de acesso;
R.HS583	Suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha do *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado ou CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
R.HS584	Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKLCS#12;
R.HS585	Suportar a solicitação de emissão de certificados a uma autoridade certificadora de confiança (*enrollment*) via SCEP (*Simple Certificate Enrollment Protocol*) ou CSR (*Certificate Signing Requests*);
R.HS586	Suportar a leitura e verificação de CRLs (*certification revogation lists*);
R.HS587	Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

Requisitos Tecnológicos (Software de Gerência)	
ID	**Descrição**
R.SG1	A solução de gerência deverá ser separada dos *gateways* de segurança. Esta irá gerenciar as políticas de segurança de todos os *firewalls* vinculados e funcionalidades solicitadas. Deverá ainda armazenar *logs* e produzir relatórios de forma unificada;
R.SG2	A solução deve, preferencialmente, ser do tipo "*appliance virtual*" – solução de *software* baseada em máquina virtual, conforme os padrões estabelecidos pelo DMTF (*Distributed Management Task Force*), ou sistema operacional desenvolvido pelo próprio fabricante da solução de gerenciamento que possa ser instalado e executado em ambiente virtual – compatível com *VMWare vSphere* 6 ou superior. Será aceito combinação de dois *appliances virtuais* para compor solução de gerenciamento centralizado e armazemanento de logs;
R.SG3	Caso seja ofertada solução em *appliance* físico, a solução deve atender a todas as exigências previstas para a solução fornecida em *appliance virtual*, devendo ser fornecido com configuração de CPU e memória (RAM e *Flash*) suficiente para implementação de todas as funcionalidades descritas nesta especificação, simultaneamente;
R.SG4	Caso a solução ofertada seja em *appliance* físico a utilização de memória e CPU não deve exceder 70% de utilização;

R.SG5	Caso seja ofertada solução em *appliance* físico, esta deverá ser fornecida em alta disponibilidade, de modo que a falha de um equipamento não cause a indisponibilidade da solução de gerenciamento;
R.SG6	Deve estar licenciada e permitir a gerência centralizada de todos os equipamentos e contextos virtuais que compõem a solução de alta disponibilidade;
R.SG7	Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertada, no mínimo, a de capacidade de armazenamento local de *logs* indexados por no mínimo 100 dias, assim como deve suportar uma capacidade mínima de 3TB de armazenamento total de *logs* indexados;
R.SG8	Deve estar licenciada para o limite máximo de usuários objetos, regras de segurança, NAT e endereços IP suportados pela solução;
R.SG9	Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contexto que compõem a solução de alta disponibilidade;
R.SG10	Deve permitir a criação de distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os *clusters*;
R.SG11	Suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de *Next Generation Firewall*, filtragem de URLs, monitoração de *logs*, *debugging*, *troubleshooting*;
R.SG12	Deve possuir a capacidade de definir administradores com diferentes perfis de acessos. Os perfis de acesso devem ser no mínimo de leitura/escrita e somente leitura;
R.SG13	Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterar configurações, ler configurações, etc.;
R.SG14	Deve permitir a delegação de funções de administração;
R.SG15	Suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente;
R.SG16	Deve registar em *log* de auditoria as ações dos usuários administradores;
R.SG17	Suportar a identificação e utilização de usuários nas políticas de segurança;
R.SG18	Suportar agrupamento lógico de objetos (*object grouping*) para criação de regras;
R.SG19	Deve incluir a opção de segmentar a base de regra utilizando rótulos ou Títulos de seção para melhor organizar a política;
R.SG20	Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deverá ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos deverão permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas;
R.SG21	Deve contabilizar a utilização (*hit counts*) ou o volume de dados trafegados correspondentes a cada regra de filtragem (*Access Control Entry*) individualmente;
R.SG22	Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês ano, dia da semana e hora);
R.SG23	Deve permitir distribuição centralizada de pacotes de atualização;
R.SG24	Deve ser capaz de testar a conectividade dos equipamentos gerenciados;

R.SG25	Suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos;
R.SG26	Deve permitir localizar em quais regras um objeto está sendo utilizado;
R.SG27	Deve prover funcionalidade para análise e auditoria de regras com capacidade de detectar regras conflitantes, regras equivalentes ou um conjunto de regras que possa ser condensado em uma única regra;
R.SG28	Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico);
R.SG29	Suportar a geração de alertas automáticos via e-mail, SNMP ou *syslog*;
R.SG30	Suportar *rollback* de configuração para a última configuração salva;
R.SG31	Deve permitir validar as regras antes de aplica-las;
R.SG32	Deve permitir a visualização e comparação das configurações atual, anterior e antigas;
R.SG33	Deve permitir a exportação automática e agendada de *logs* via SCP;
R.SG34	Deve possuir relatórios de utilização dos recursos por, no mínimo, aplicação ou categoria, usuários, IP de origem/destino;
R.SG35	Deve possuir visualização sumarizada de todas as aplicações, ameaças e URL's que foram identificadas e controladas pela solução;
R.SG36	Deve permitir a criação de relatórios customizados;
R.SG37	Deve possibilitar a filtragem dos *logs* do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário;
R.SG38	Deve possuir relatório com informações consolidadas sobre as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços, ou mais frequentes ataques e ameaças de segurança, detectados com suas origens e destinos, os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet, os usuários maiores consumidores de banda de Internet, os sítios na Internet mais visitados;
R.SG39	Deve ser gerado relatório caso a abertura do *link* pela *Sandbox* o identifique como site hospedeiro de *exploits* ou *malware*;
R.SG40	Para ameaças trafegadas em protocolo SMTP, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
R.SG41	A *Sandbox* deve prover informações sobre as ações do *malware* na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo *malware*, gerar assinatura de antivírus e *Anti-spyware* automaticamente, definir URL's não confiáveis utilizadas pelo novo *malware* e prover informações sobre o usuário infectado;
R.SG42	Deve permitir a geração automática e agendada dos relatórios;
R.SG43	Deverá permitir seu gerenciamento por CLI (*Command Line Interface*), via SSH, *Web* GUI utilizando HTTPS ou console gráfica proprietária do fabricante;
R.SG44	Deve possuir mecanismo de ajuda de comandos via SSH, facilitando a localização e parâmetros dos mesmos;
R.SG45	Deve possuir console de *log* onde é possível visualizar os *logs* em tempo real, permitindo ao administrador realizar as devidas análises para fins de *troubleshooting*;

R.SG46	Deverá prover fácil administração na aplicação das políticas para os *gateways*, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, que pode ser aplicada nos *gateways* remotos em uma única sessão, evitando qualquer tipo de retrabalho de configuração e reaplicação de regra;
R.SG47	Deve possuir console de visualização da topologia dos *firewalls* gerenciados, de forma centralizada;
R.SG48	Deve prover informações do status de todos os túneis VPN, incluindo: • Túneis permanentes e seu estado de conexão; • Túneis e suas comunidades; • Usuários conectados utilizando a VPN "*client-to-site*";
R.SG49	Deverá prover informações gerais de cada *gateway* como volume de pacotes aceitos, conexões concorrentes, novas conexões e licenciamento;
R.SG50	O monitoramento deverá ser capaz de monitorar todos os usuários remotos conectados;
R.SG51	Deve ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, assim como registrar e alertar quando o túnel VPN estiver desconectado;
R.SG52	Deve possuir recurso de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras (*shadowing*);
R.SG53	Deve suportar a programação de relatórios automáticos;
R.SG54	Deverá permitir exportar o resultado das análises de *malwares* de dia Zero em PDF a partir da própria interface de gerência;
R.SG55	Deverá permitir o *download* dos *malwares* identificados a partir da própria interface de gerência;
R.SG56	Deverá permitir visualizar os resultados das análises de *malwares* de dia Zero nos diferentes sistemas operacionais suportados;
R.SG57	Deverá permitir informar ao fabricante quanto a suspeita de ocorrências de falso positivo e falso negativo na análise de *malwares* de dia Zero a partir da própria interface de gerência;

Requisitos de Instalação e Configuração	
ID	**Descrição**
R.IC1.	A instalação dos equipamentos deverá ser realizada no *DataCenter* do Tribunal Superior do Trabalho;
R.IC2.	Todo ferramental necessário para execução dos serviços de instalação, configuração inicial, incluindo *softwares*, equipamentos ou ferramentas, bem como eventuais materiais necessários para ligações temporárias, são de inteira responsabilidade da CONTRATADA;
R.IC3.	A CONTRATANTE disponibilizará o espeço no *DataCenter*, assim como a infraestrutura elétrica até a posição onde será instalados equipamentos;
R.IC4.	O equipamento deverá ser instalado na última versão de *firmware* disponível pelo fabricante;

R.IC5.	Entende-se por configuração inicial para efeito deste estudo: • Elaboração em conjunto com a equipe técnica do TST, de projeto de configuração, segundo as melhores práticas do fabricante e considerando as demandas e características dos serviços do CONTRATANTE; • Realização da configuração inicial do equipamento ofertado, segundo projeto, e conforme padrão de endereçamento IP a ser fornecido pelo CONTRATANTE; • Realização de migração e adequação das regras vigentes no CONTRATANTE, de forma automatizada;

Requisitos de Treinamento (Capacitação)	
ID	**Descrição**
R.T1	A Contratada deverá fornecer treinamento oficial do fabricante, podendo ocorrer nas dependências do TST ou em local próprio indicado pela Contratada;
R.T2	Todos os custos envolvidos com o treinamento deverão ser de responsabilidade da Contratada, incluindo material didático, hospedagem e passagem (dos alunos), caso não seja realizado em Brasília;
R.T3	O treinamento poderá ser oferecido na modalidade EaD;
R.T4	O treinamento deverá ser focado na aprendizagem e no desenvolvimento de habilidades práticas necessárias para configurar e gerenciar o ambiente;
R.T5	O treinamento deverá ter carga horária de, no mínimo, 40 (quarenta) horas;
R.T6	Caso haja necessidade de carga horária superior a 40 (quarenta) horas, deve haver um intervalo de, no mínimo 1 (uma) semana e no máximo 3 (três) semanas entre os módulos;
R.T7	Os cursos deverão habilitar o participante a gerenciar a solução e a realizar configurações referentes às funcionalidades especificadas nos requisitos tecnológicos.
R.T8	Os certificados deverão ser entregues no prazo de 10 (dez) dias corridos contados após o término do treinamento, sem ônus adicional para a CONTRATANTE;
R.T9	Deverá ser fornecido treinamento para 5 (cinco) servidores indicados pelo CONTRATANTE

Requisitos Legais, Sociais e Ambientais	
ID	**Descrição**
R.LSA01	A empresa deverá estar habilitada juridicamente (art. 28 da Lei n.º 8.666/93) e em regularidade fiscal e trabalhista (art. 29 da Lei n.º 8.666/93).
R.LSA02	Decreto Nº 2.271 de 7 de Julho de 1997, que dispõe sobre a contratação de serviços pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências
R.LSA03	Resolução CNJ nº 182/2013, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça.
R.LSA04	Decreto-lei N.º 5.452, de 1º de Maio de 1943, que define a Consolidação das Lei do Trabalho.
R.LSA05	Súmula nº 269 do TCU que estabelece que nas contratações para a prestação

	de serviços de Tecnologia da Informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis mínimos de serviço.
R.LSA06	Cumprir o disposto no inciso XXXIII do art. 7.º da Constituição Federal de 1988, quanto ao emprego de menores.
R.LSA07	Promover a correta destinação dos resíduos resultantes da prestação do serviço, tais como peças substituídas, embalagens, entre outros, observando a legislação e princípios de responsabilidade socioambiental como a Política Nacional de Resíduos Sólidos (Lei n.º 12.305/2010) e o Guia de Contratações Sustentáveis da Justiça do Trabalho (Resolução n.º 103/2012 do Conselho Superior da Justiça do Trabalho).
R.LSA08	Prever a destinação ambiental adequada das pilhas e baterias usadas ou inservíveis, segundo disposto na Resolução CONAMA nº 257, de 30 de junho de 1999.
R.LSA09	Os equipamentos devem obrigatoriamente estar em conformidade com o artigo 55 da Resolução 715 de 23 de outubro de 2019, emitida pela ANATEL;
R.LSA10	Possuir certificação de conformidade sustentável de acordo com os padrões EPA (*Enviromental Protection Agency*) ou similar, tais como, *EnergyStar*, *RoHS* (*Restriction on Harzadous Substances*), WEEE (*Waste Electrical and Eletronic Equipament*) ou EMI *Certifications* FCC *part* 15, CE, EN55022, EN55024.

Requisitos de Manutenção	
ID	**Descrição**
R.M1	Elaboração do plano de implementação dos novos equipamentos e *software* de gerenciamento, envolvendo: • Instalação dos equipamentos novos, sem prejuízo da operação da rede atual;
R.M2	Documentação de Planejamento e implementação detalhada da solução;
R.M3	Substituição dos *firewalls* existentes;
R.M4	Configuração das funcionalidades Next Generation *Firewall*, IPS, proteção avançada contra ameaças, QoS, controle de aplicativos e VPN IPSEC;
R.M5	Migração das políticas de segurança existentes;
R.M6	Criação dos usuários administradores;
R.M7	Criação de perfis de usuários da VPN IPSEC;
R.M8	Customização de regras de acesso de acordo com as necessidades do TST;
R.M9	Integração com o *Active Directory*;
R.M10	Realização de *backup* das configurações;
R.M11	Operação Assistida de Funcionamento da Solução, que consiste da disponibilização de um técnico residente, das 8h às 17h, com intervalo para almoço, no endereço do Contratante, devidamente identificado, para sanar quaisquer dúvidas e problemas que ocorrerem na operação da solução, durante 3 dias. Este técnico deverá ser certificado pelo fabricante do equipamento.
R.M12	Testes de Aceite e Funcionamento;
R.M13	Fornecimento da documentação de todo o projeto;
R.M14	A instalação dos equipamentos deverá ser efetuada pela Contratada ou Fabricante, conforme orientação do Serviço de Infraestrutura do Órgão da JT Contratante, observados os seguintes itens: • Todos os componentes necessários para o correto funcionamento dos equipamentos ofertados devem ser fornecidos pela Contratada;

R.M15	Caberá à Contratada ou Fabricante a montagem dos equipamentos no RACK já existente.

Requisitos de Prazo	
ID	**Descrição**
R.P1	A entrega total dos equipamentos e *software*, objeto da ordem de fornecimento deverá ocorrer em até 60 (sessenta) dias corridos e contados após a assinatura do Contrato;
R.P2	A instalação, configuração e migração das regras deverá ocorrer em até 30 dias após a entrega dos equipamentos;
R.P3	O fornecedor contratado deverá assegurar a disponibilidade da solução conforme os **Níveis Mínimos de Serviço (NMS)**, através de número telefônico específico para o fim ou e-mail na forma abaixo estabelecida:
R.P4	No momento da abertura do chamado, será informada a prioridade para o atendimento de acordo com as seguintes definições: • **Prioridade 1 (Crítica)**: Este Nível de severidade é aplicado em situações de emergência ou problema crítico, caracterizado pela existência de ambiente paralisado. • **Prioridade 2 (Alta)**: Este nível de severidade é aplicado em situações de alto impacto, incluindo os casos de degradação severa de desempenho da solução. Também se aplica a esta severidade casos onde um *appliance* para de funcionar, ocasionando a perda da alta disponibilidade da solução. Outros exemplos para esta severidade: Perda de redundância, reinicialização de módulos, slots ou portas com defeitos, perda de funcionalidades. • **Prioridade 3 (Média)**: Este nível de severidade é aplicado em situações de baixo impacto ou de problemas que se apresentam de forma intermitente. • **Prioridade 4 (Baixa)**: Este nível de severidade é aplicado em situações de dúvidas técnicas em relação ao uso ou à implementação da solução.

R.P5

PRAZOS	PRIORIDADE			
	1 (Crítica)	2 (Alta)	3 (Média)	4 (Baixa)
Início do atendimento	Até 30 minutos após a abertura do chamado	Até 1 hora após a abertura do chamado	Até 4 horas após a abertura do chamado	Até 8 horas após a abertura do chamado
Solução Definitiva	Em até 6h do início do atendimento	Em até 12h do início do atendimento	Em até 24h do início do atendimento	Em até 72h do início do atendimento
Tolerância mensal de	0	1	2	2

	descumprimentos | | | | |
R.P6	Em caso onde ocorram descumprimentos de NMS que se enquadre nos valores de tolerância acima informados, a empresa será notificada e advertida do não cumprimento do acordo de nível de serviço;
R.P7	Caso existam ocorrências que ultrapassem os níveis de tolerância informados na tabela acima, serão aplicadas as seguintes penalidades:
R.P8	Multa: a) 1% (um por cento) ao dia sobre o valor referente ao respectivo item, no caso de atraso injustificado para a entrega dos equipamentos e do *software* de gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato; b) 1% (um por cento) ao dia sobre o valor referente aos itens a serem instalados, no caso de atraso injustificado para conclusão do Serviço de Instalação dos Equipamentos e do *Software* de Gerenciamento, limitado à incidência de 30 (trinta) dias, quando será considerada a inexecução do contrato; c) Para o item 1, 2% (dois por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 1 (CRÍTICA); d) Para o item 1, 1% (um por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 2 (ALTA); e) Para o item 1, 0,5% (meio por cento) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (MÉDIA); f) Para o item 1, 0,25% (vinte e cinco décimos percentuais) por hora sobre o valor do item, na hipótese de atraso ou interrupção injustificado nos prazos estabelecidos para o atendimento e/ou solução dos chamados abertos com nível de Prioridade 3 (BAIXA);
R.P9	Os atendimentos às solicitações de severidade crítica, alta ou média deverão ser realizados nas instalações do Contratante (*on-site*) e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo Contratante, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao Contratante;
R.P10	Os atendimentos às solicitações de severidade média poderão ser realizados remotamente ou nas instalações do Contratante (*on-site*), conforme o caso, e não poderão ser interrompidos até o completo restabelecimento dos serviços, salvo em casos excepcionais, autorizados pelo Contratante, mesmo que se estendam por períodos noturnos, sábados, domingos e feriados. Tal situação não implicará em custos adicionais ao Contratante;
R.P11	Os atendimentos às solicitações de severidade baixa poderão ser realizados remotamente, de segunda à sexta-feira, respeitando o horário de funcionamento do Contratante. Caso seja necessário o atendimento nas instalações do Contratante (*on-site*), tal situação não implicará custos adicionais ao Contratante;

R.P12	A interrupção do atendimento de uma solicitação, de quaisquer das severidades, por parte da Contratada sem prévia autorização da Equipe Técnica do Contratante será caracterizada como um descumprimento mensal para efeitos de aplicação dos descontos apresentados no requisito R.P2;
R.P13	Concluído o atendimento, a Contratada comunicará o fato à Equipe Técnica do Contratante e solicitará autorização para o fechamento do chamado. Caso o Contratante não confirme o pleno atendimento da solicitação, o chamado permanecerá aberto até que seja efetivamente atendido. Nesse caso, a Equipe Técnica fornecerá as pendências relativas à solicitação em aberto;
R.P14	O Contratante encaminhará formalmente à Contratada, quando da reunião de apresentação inicial, a relação nominal da Equipe Técnica autorizada a abrir e fechar solicitações de suporte técnico;
R.P15	Todas as solicitações de atendimento serão registradas pelo fiscal do contrato e pela Contratada, para acompanhamento e controle da execução do contrato: a) A Contratada apresentará um Relatório de Atendimento, enviado por meio de correio eletrônico, contendo datas e horas de chamada, de início e de término do atendimento, descrição da necessidade de atendimento, e as providências adotadas e toda e qualquer informação pertinente ao chamado após o encerramento do mesmo; b) A equipe técnica do Contratante informará à Contratada quanto ao recebimento e aceite do Relatório de Atendimento;
R.P16	Na abertura do chamado a Contratada deverá fornecer o número de protocolo e o horário de abertura e encaminhar mensagem de correio eletrônico com tais informações para os endereços dos fiscais do contrato em até meia hora após o registro, procedimento que servirá como evidência em caso de contestação de penalidades. O cálculo para aferição da desconformidade do tempo de resposta considerará o tempo de resposta descrito nos níveis mínimos de serviço;
R.P17	Para fins de aferição dos níveis mínimos de serviço, ao final, o chamado será considerado: completamente atendido ou não atendido, não havendo possibilidade de atendimento parcial;
R.P18	Quando a solução depender de ações do Contratante o tempo de solução do chamado deve ser pausado até a conclusão da parte que não cabe a contratada, depois continuar de onde havia parado antes da solicitação do outro ator no processo;
R.P19	Todas as ações provenientes de um chamado deverão ser amplamente comunicadas ao Contratante. Sendo que o Contratante deverá ser comunicado no mínimo em dois momentos, no início e no final de cada atendimento;
R.P20	Os níveis mínimos de serviço serão aferidos mensalmente e eventuais descumprimentos atestados no Termo de Recebimento Definitivo;
R.P21	Toda indisponibilidade causada pela solução contratada, poderá gerar multa de acordo com o NMS descrito acima;
R.P22	Faculta-se à Contratada substituir temporariamente um componente defeituoso por outro de mesmas características técnica ou superior: a) A Contratada deverá realizar a substituição definitiva do referido componente no prazo de 30 (trinta) dias corridos; b) A substituição definitiva de componentes, caso necessário, deverá ser feita por itens novos e para primeiro uso.
R.P23	O Contratante poderá autorizar a substituição, em caráter definitivo, o componente já instalado, por um novo e para primeiro uso, em perfeito estado de funcionamento, no prazo de 30 (trinta) dias corridos, em quaisquer dos

	seguintes casos: a) Ocorrência de 3 (três) ou mais defeitos que comprometam o seu perfeito funcionamento, dentro de um período qualquer de 30 (trinta) dias corridos; e b) Somatório dos tempos de paralisação de quaisquer componentes que ultrapasse 15 (quinze) horas dentro de um período qualquer de 30 (trinta) dias corridos.
R.P24	Qualquer substituição de componente, temporária ou definitiva, só será permitida após prévia avaliação técnica e autorização por parte da Equipe Técnica do Contratante.

Requisitos de Segurança da Informação	
ID	**Descrição**
R.SI01	O acesso às instalações do Contratante onde serão realizados os serviços deverá ser controlado e permitido somente às pessoas autorizadas.
R.SI02	A Contratada deverá substituir imediatamente aquele profissional que seja considerado inconveniente à boa ordem ou que venha a transgredir as normas disciplinares do Contratante.
R.SI03	Os profissionais disponibilizados pela Contratada para a prestação dos serviços deverão estar identificados com crachá de identificação da mesma, estando sujeitos às normas internas de segurança do Contratante, inclusive àqueles referentes à identificação, trajes, trânsito e permanência em suas dependências.
R.SI04	A Contratada deverá acatar e obedecer às normas de utilização e segurança das instalações do Contratante.
R.SI05	Respeitar o sistema de segurança do Contratante e fornecer todas as informações relacionadas ao equipamento quando solicitadas por ele.
R.SI06	A Contratada deverá garantir a segurança das informações do Contratante e se comprometer em não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido do Contratante no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

Requisitos de Garantia	
ID	**Descrição**
R.G1	A garantia será aquela, usualmente fornecida pelo fabricante acrescida dos Níveis de Serviço Exigidos (NSE) e demais condições estabelecidas neste Estudo Técnico;
R.G2	A garantia para todos os equipamentos será de 60 (sessenta) meses.
R.G3	Todos os itens deverão possuir suporte ilimitado para abertura de chamados junto ao Fabricante;
R.G4	A abertura de chamados será efetuada por correio eletrônico e por telefone 0800 ou com número de DDD igual ao da localidade do contratante. Em ambos os casos, o atendimento deve ser efetuado em Língua Portuguesa.
R.G5	O início de atendimento e da resolução do serviço de garantia será a hora da comunicação feita pelo Contratante à Contratada, conforme sistema de registro do próprio do solicitante.
R.G6	Na abertura do chamado, a Contratada deverá fornecer um número de registro para acompanhamento de cada equipamento.

R.G7	O serviço de suporte técnico deverá ser prestado de forma ininterrupta no regime 24x7 (vinte e quatro horas durante sete dias por semana), inclusive em feriados e deverá cobrir todo e qualquer defeito e/ou problema apresentado nos equipamentos ou serviços da solução de *firewall*, peça ou componente, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias.
R.G8	A manutenção será *on-site* (procedimentos realizados no local de instalação) sempre com acompanhamento de um servidor do quadro do Tribunal;
R.G9	Quando não for possível a execução do serviço, em razão da ausência de servidor para acompanhamento, deve o técnico anotar este fato no relatório junto com o tempo de espera;
R.G10	Atualizações para novas versões e releases de *software* lançadas durante a vigência do contrato;
R.G11	Atualizações periódicas de todas as bases de assinaturas dos componentes;
R.G12	Suporte para a instalação e configuração das novas versões e *releases* de *software* lançadas durante a vigência do contrato;
R.G13	Apresentação de solução para as solicitações do TST em até 8 (oito) horas, exceto em caso de bug de *software* que deverá ser de 4 (quatro) horas: • Por solução entende-se o atendimento, identificação do problema e sua correção; • Em havendo necessidade de retirada do equipamento para conserto em laboratório, esta deverá substituir o equipamento defeituoso por outro, igual ou superior, em regime 24x7 (vinte e quatro horas durante sete dias por semana), inclusive em feriados com entrega no próximo dia útil, para chamados abertos até às 14h. Após esse horário, o chamado passa a ser contado a partir do próximo dia; • Em caso de defeitos de *software* que necessitem de desenvolvimento de correções pelo fabricante, o prazo deverá ser acordado com o TST;
R.G14	O tempo de indisponibilidade será calculado pela diferença entre a abertura da solicitação e o aceite da correção do problema;
R.G15	Não será considerada indisponibilidade de equipamentos quando ocorrer uma ou mais das seguintes condições: • Quando for caracterizado o uso indevido e/ou mau uso, comprovado por relatório técnico aceito pelo Serviço de Infraestrutura (CITEC); • Quando ocorrer falta de energia elétrica; e • Quando o TST não disponibilizar o equipamento para a manutenção *on-site*, devendo o técnico observar no relatório o tempo de espera. • Quando o Tribunal não disponibilizar técnico para acompanhamento da manutenção.
R.G16	A indisponibilidade cessará quando: • O equipamento for colocado em funcionamento pela Contratada, após testes de validação, acompanhamento e assinatura do Relatório de Atendimento Técnico pelo TST; • O equipamento for substituído por *backup* igual ou superior, quando necessária a retirada para conserto em laboratório; • Equipamentos substituídos por *backup* têm um prazo de 45 (quarenta e cinco) dias corridos para serem devolvidos ao TST, devidamente reparados; • Quando não houver a possibilidade de conserto do equipamento, este

	deverá ser substituído por equipamento novo, de características iguais ou superiores às do equipamento em questão; • Se o *backup* for um equipamento novo, ele poderá ser aceito na substituição, a critério do TST; • A substituição só será aceita com relatório detalhado sobre as causas e motivos do mau funcionamento, assim como a indicação do motivo da impossibilidade de conserto.
R.G17	Substituição de componentes: • Em caso de quebra, mau funcionamento, queda de desempenho ou qualquer outro fato causado por defeitos em componentes dos equipamentos, deverá ser realizado a troca dos componentes por novos, do mesmo modelo ou tecnicamente superiores, homologados pelo fabricante. Não serão aceitos componentes recondicionados ou usados anteriormente.

Poder Judiciário
Justiça do Trabalho
Tribunal Superior do Trabalho

TERMO DE GARANTIA DO OBJETO

ANEXO II DO CONTRATO PE-031/2020 - AQUISIÇÃO E INSTALAÇÃO DE SOLUÇÃO DE SEGURANÇA FIREWALL. (PROCESSO TST N.º 501.233/2020-5)

1. DA GARANTIA

1.1. A **[NOME DA EMPRESA]**, doravante denominada Concedente, garante os produtos por ela fabricados e/ou fornecidos, pelo período de 60 (sessenta) meses, incluída a garantia legal, contados a partir do recebimento definitivo do objeto do contrato.

1.2. Os três primeiros meses compreendem a garantia legal, e os cinquenta e sete meses, compõem a garantia contratual, que é complementar àquela.

1.3. A garantia compreende a substituição dos equipamentos, peças, componentes e a mão-de-obra no reparo de defeitos de fabricação.

1.4. Somente um técnico autorizado pela Concedente está habilitado a reparar defeitos cobertos pela garantia, mediante apresentação da nota fiscal pelo usuário do produto.

2. DA ASSISTÊNCIA TÉCNICA

2.1. A Concedente deverá prestar os serviços de assistência técnica e efetuar os consertos e/ou substituições que se fizerem necessários, durante o período de garantia, nos prazos fixados pelo TST, que serão contados do recebimento da solicitação formal feita pela Fiscalização.

2.1.1. A Concedente deverá cumprir os requisitos de garantia estabelecidos no Anexo I deste Contrato.

2.1.2. Por ocasião da entrega do objeto será requerido o fornecimento da documentação de suporte técnico e manutenção em garantia, contendo as informações necessárias para abertura dos chamados por telefone e por correio eletrônico (códigos de acesso, números de telefone, endereços de correio eletrônico, códigos de identificação do cliente, etc.).

2.1.3. A Concedente deverá assegurar a garantia dos equipamentos, seja por meio da rede mantida pelo próprio fabricante ou por meio de rede por ele credenciada, sendo, em todo caso, capaz de atender no local de entrega dos equipamentos com, no mínimo, um estabelecimento técnico.

2.2. A Concedente assumirá toda e exclusiva responsabilidade pela qualidade dos itens fornecidos, não se admitindo que sejam atribuídos a técnicos ou a fornecedores os ônus de quaisquer problemas que porventura venham a ocorrer.

2.3. Os serviços de assistência técnica deverão ser prestados por técnicos credenciados e pagos pela Concedente, correndo por sua conta e responsabilidade o deslocamento desses técnicos aos locais de instalação e/ou a movimentação do mobiliário à oficina.

2.4. Caso o atendimento do chamado e/ou a execução do serviço de assistência técnica não sejam realizados dentro do prazo, a Concedente ficará sujeita à multa estabelecida neste termo de garantia e no edital da licitação correspondente.

2.5. A Concedente garante a existência de peças e componentes para reposição durante o período de garantia.

3. AS GARANTIAS LEGAL E/OU CONTRATUAL NÃO COBREM:

3.1. Produtos ou peças que tenham sido danificados em consequência de remoção ou manuseio por pessoas não autorizadas;

3.2. Peças sujeitas ao desgaste natural, descartáveis ou consumíveis, bem como a mão-de-obra utilizada na aplicação das peças e as consequências advindas dessas ocorrências.

4. AS GARANTIAS LEGAL E/OU CONTRATUAL FICAM AUTOMATICAMENTE INVALIDADAS SE:

4.1. O produto tiver sofrido alterações ou modificações estéticas e/ou funcionais, bem como tiver sido realizado conserto por pessoas ou entidades não credenciadas pela Concedente;

4.2. Os defeitos forem provocados pela utilização de material ou peças fora das especificações.

5. SANÇÃO POR DESCUMPRIMENTO DAS OBRIGAÇÕES CONTRATUAIS

5.1. O atraso injustificado na conclusão dos serviços implicará multa correspondente a 1% (um por cento) por dia de atraso, calculado sobre o valor do objeto em atraso, até o limite de 30% (trinta por cento) do respectivo valor total.

5.2. Na hipótese mencionada no item anterior, o atraso injustificado por período superior a 30 (trinta) dias caracterizará o descumprimento total da obrigação, punível com a sanção prevista no item 18.1 do edital da licitação, como também a inexecução total do contrato, caso esteja vigente.