TERMO DE CONTRATO - PE 11636/2025-TRT12
(Ata RP nº 06/2025)

Contrato TRT3 nº 10-002-2026
PROAD n. 701/2026

Termo de Contrato de prestação de serviços de garantia e atualização de assinaturas de proteção e suporte técnico, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewall*, incluindo *software* de administração e gerência integrada, que, entre si, celebram o **TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO** e a empresa **NTSEC - SOLUÇÕES EM TELEINFORMÁTICA LTDA.**

CONTRATANTE: A União, por meio do **TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO**, inscrito no CNPJ sob o n. 01.298.583/0001-41, com sede na Av. Getúlio Vargas, 225, em Belo Horizonte – MG, neste ato representado por sua Diretora-Geral, Patrícia Helena dos Reis, brasileira, casada, portadora da Carteira de Identidade M 5.564.741, expedida pela Secretaria de Segurança Pública de Minas Gerais, inscrita no Cadastro de Pessoas Físicas do Ministério da Fazenda sob o nº 911.765.736-91, residente e domiciliada em Belo Horizonte – MG, conforme competência que lhe foi delegada pela Portaria TRT/GP 03/2026, de 02 de janeiro de 2026, em decorrência da nomeação constante da Portaria TRT/GP 07/2024, de 02 de janeiro de 2024, disponibilizadas no Diário Eletrônico da Justiça do Trabalho de 30 de dezembro de 2025 e de 29 de dezembro de 2023, respectivamente.

CONTRATADA: A empresa **NTSEC - SOLUÇÕES EM TELEINFORMÁTICA LTDA.**, pessoa jurídica de direito privado, devidamente inscrita no CNPJ sob o nº 09.137.728/0001-34, estabelecida no SCN, Quadra 05 Bloco A, nº 50, Torre Norte, Sala 617, Edifício Brasília Shopping - Asa Norte, em Brasília – DF, CEP: 70.715-900, neste ato representada por sua Sócia-Administradora, Patrícia Angelina da Conceição, portadora da carteira de identidade n° 48.453.021-5, expedida pela SSP/SP e inscrita no CPF/MF sob o n° 346.994.838-01, conforme Contrato Social.

Os CONTRATANTES resolvem celebrar o presente contrato, mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA – DO ATO AUTORIZATIVO

A celebração deste contrato decorre de despacho exarado pelo Exmo. Desembargador do Trabalho-Presidente do Tribunal Regional do Trabalho da 12ª Região, que adjudicou e homologou a licitação no processo PE 11636/2025, em coparticipação com o Tribunal Regional do Trabalho da 3ª Região, processo PROAD 25880/2025.

CLÁUSULA SEGUNDA – DO OBJETO DO CONTRATO

Constitui-se objeto da presente Contratação a prestação dos serviços de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7, por 60 meses adicionais, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewal*, com alta disponibilidade, incluindo *software* de administração e gerência integrada.

Grupo I - Serviço de suporte e manutenção para solução de NG *Firewall* utilizada na JT	
Item	**Descrição**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7, por 60 meses adicionais, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewall*, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**

CLÁUSULA TERCEIRA – DA EXECUÇÃO DO CONTRATO

A prestação dos serviços obedecerá ao seguinte:

I – Da vigência e do prazo de execução dos serviços:

Os serviços serão executados conforme os prazos estipulados no Anexo I - Especificações Técnicas para Solução de *Next Generation Firewall* - NGFW.

II - Da vigência dos serviços de suporte:

Os serviços de suporte terão seu prazo de vigência conforme descrito no Anexo I - Especificações Técnicas para Solução de *Next Generation Firewall* - NGFW.

III - Da garantia de equipamentos e serviços:

a) para equipamentos já instalados, a garantia de 60 (sessenta) meses adicionais – prevista na Cláusula Segunda deste ajuste - deve iniciar em até 10 (dez) dias após a comunicação da assinatura do contrato;

IV - Da especificação completa da solução escolhida:

Devido à complexidade das especificações completas da solução, as informações referentes a esta seção estarão disponíveis no Anexo I - Especificações Técnicas para Solução de *Next Generation Firewall* - NGFW.

V - Da relação entre demanda prevista e quantidade contratada:

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall utilizada na JT			
Item	**Descrição**	**Unidade**	**Quantidade**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7, por 60 meses adicionais, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewall*, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	*Cluster*	1

§ 1º - Para esta Contratação, será adotada a definição de *cluster* como o conjunto de dois, ou mais, equipamentos *appliances* compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de *Next Generation Firewall*.

VI - Da identificação do código CATSER:

a) **Item 1** - Suporte e Garantia a Equipamentos NG *Firewall*

Código CATSER: 27740
Nome do Serviço: Serviços de garantia de equipamentos de TIC.

VII – Da sustentabilidade:

- Não foram identificados requisitos relacionados à sustentabilidade para o item contratado.

VIII - Dos Níveis Mínimos de Serviço:

- Não se estabelecem níveis mínimos para a prestação dos serviços contratados neste Ajuste.

IX - Da qualificação dos profissionais:

a) para a comprovação das certificações, deverá ser apresentada cópia do certificado emitido pelo órgão certificador;

b) a Contratada deverá apresentar ao menos um profissional para cada certificação e um mesmo profissional poderá atender a mais de uma certificação;

c) para a comprovação do vínculo dos profissionais com a Contratada, exigidos no edital, deverão ser apresentados documentos que atestem formalmente a relação empregatícia ou de prestação de serviços;

d) a Contratada deverá apresentar a documentação de cada profissional listado, que poderá ser, alternativamente:

- cópia da Carteira de Trabalho e Previdência Social (CTPS), com as páginas de identificação do profissional e do registro do contrato de trabalho, comprovando o vínculo empregatício;
- Contrato de Trabalho assinado entre o profissional e a empresa, para vínculos empregatícios formais;
- Contrato de Prestação de Serviços, quando o profissional atuar como Pessoa Jurídica (PJ), acompanhado de documentação que comprove a regularidade da empresa do profissional;

e) a Contratada se compromete a manter o quadro de profissionais, com os vínculos comprovados, durante toda a vigência do contrato; a substituição de qualquer profissional com certificação exigida deverá ser comunicada formalmente e aprovada pela Contratante, mediante a apresentação de nova documentação que comprove a qualificação e o vínculo do novo profissional.

Parágrafo único - Os prazos de adimplemento das obrigações contratadas admitem prorrogação, nos casos de superveniência de fato excepcional ou imprevisível, estranho à vontade das partes, que altere as condições de execução do contrato; impedimento de execução do contrato por fato ou ato da Administração ou de terceiro, comprovado por documento contemporâneo à sua ocorrência, devendo a solicitação ser apresentada até o vencimento da obrigação.

CLÁUSULA QUARTA – DO RECEBIMENTO DO OBJETO

Nos termos dos incisos I e II do art. 140 da Lei nº 14.133/2021, o objeto será recebido:

1. Recebimento Provisório dos Serviços

a) a tabela abaixo especifica a periodicidade do recebimento provisório e definitivo do serviço:

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall utilizada na JT		
Item	**Descrição**	**Periodicidade**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7, por 60 meses adicionais, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewall*, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento único e antecipado - Pagamento em parcela única, antecipada.**	Único

b) o fiscal técnico irá realizar o recebimento provisório, atestando a prestação do serviço no Termo de Recebimento Provisório.

c) nesse documento, o fiscal deve realizar o registro, a análise e a conclusão acerca das ocorrências na execução do contrato no período em referência e poderá encaminhar, junto com o Termo de Recebimento Provisório, outros documentos que entender necessários para esclarecer/comprovar os fatos apresentados;

d) existindo ocorrências pendentes ou que configurem descumprimento parcial do contrato, o recebimento do objeto deve ser atestado com ressalvas. Em caso de descumprimento total do contrato, o recebimento do objeto não deve ser atestado, devendo, neste caso, o Fiscal informar a ocorrência no processo para análise pelo Gestor;

e) o Termo de Recebimento Provisório, com ou sem ressalvas, deve ser encaminhado ao gestor do contrato, junto com os demais documentos, inclusive o relatório de medição de NMS, quando previstos.

2. Recebimento Definitivo dos Serviços

a) o recebimento definitivo constitui o ato que reconhece a execução dos serviços e deve ser realizado pelo gestor do contrato; o recebimento definitivo ocorrerá com a mesma periodicidade do recebimento provisório;

b) no caso de serviços continuados com pagamento mensal, o recebimento definitivo deverá ocorrer mensalmente, ainda que com ressalvas;

c) para realizar o recebimento definitivo, o gestor deve:

c.1) realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à contratada, por escrito, as respectivas correções;

c.2) caso o contrato preveja Instrumento de Medição de Resultados (IMR), caberá ao gestor, com base no relatório apresentado pelo fiscal do contrato, analisar se o desempenho e a qualidade do serviço prestado estão em consonância com os níveis mínimos e realizar o redimensionamento de valores a serem pagos, caso constatada alguma inconformidade, pela aplicação de fator redutor;

c.3) emitir termo próprio para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e na documentação apresentados, e;

c.4) comunicar à Contratada para que emita a nota fiscal ou fatura com o valor exato dimensionado pela fiscalização com base no IMR, quando for o caso;

d) verificada alguma ocorrência no período correspondente aos serviços atestados que possa autorizar penalização da contratada, o gestor deve realizar o recebimento definitivo, ainda que com ressalvas, e encaminhar o processo à apreciação superior para análise dos efeitos quanto a pagamento e abertura de processo administrativo;

e) o gestor deve inserir o Termo de Recebimento Definitivo no PROAD, promover o aceite da Nota Fiscal no SIGEO e encaminhar o expediente para pagamento. A nota fiscal deverá ser inserida no SIGEO pelo fornecedor.

CLÁUSULA QUINTA – DA VIGÊNCIA

O contrato terá vigência a partir da data de assinatura até a conclusão do prazo de execução definido na cláusula terceira, sendo prorrogado automaticamente nos casos do art. 111 da Lei nº 14.133/2021.

§ 1º – O prazo de vigência não se confunde com o prazo de execução de que trata a cláusula terceira.

§ 2º – O Contratante convocará a Contratada para assinar termo aditivo ou instrumento equivalente dentro do prazo de 5 (cinco) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas na Lei n° 14.133/2021.

§ 3º – O início da contagem do prazo a qual refere-se o parágrafo anterior dar-se-á a partir do primeiro dia útil seguinte ao aviso eletrônico ou comunicação escrita encaminhada à Contratada. O ato convocatório será realizado preferencialmente via *e-mail*.

CLÁUSULA SEXTA – DAS PRERROGATIVAS DO CONTRATANTE

São as seguintes as prerrogativas da Administração, conferidas em razão do regime jurídico dos contratos administrativos instituídos pelo art. 104 da Lei nº 14133/2021, em relação a eles:

I – Modificá-los, unilateralmente, para melhor adequação às finalidades de interesse público, respeitados os direitos do contratado.

II – Extingui-los, unilateralmente, nos casos especificados nesta Lei.

III – Fiscalizar sua execução.

IV – Aplicar sanções motivadas pela inexecução total ou parcial do ajuste.

V – Ocupar provisoriamente bens móveis e imóveis e utilizar pessoal e serviços vinculados ao objeto do contrato nas hipóteses de:

a) risco à prestação de serviços essenciais;

b) necessidade de acautelar a apuração administrativa de faltas contratuais pelo contratado, inclusive após extinção do contrato.

§ 1º As cláusulas econômico-financeiras e monetárias dos contratos não poderão ser alteradas sem prévia concordância do contratado.

§ 2º Na hipótese prevista no inciso I do *caput*, as cláusulas econômico-financeiras do contrato deverão ser revistas para que se mantenha o equilíbrio contratual.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

A Contratada se obriga a:

§ 1º – Das obrigações gerais e específicas:

a) proceder, no início da contratação, ao seu cadastramento no SIGEO-JT – Sistema Integrado de Gestão Orçamentária e Financeira da Justiça do Trabalho - Módulo Execução Orçamentária, bem como responsabilizar-se pela gestão de seus dados;

b) responsabilizar-se pela juntada, por meio do referido Sistema, dos documentos de cobrança/documentos fiscais (notas fiscais/faturas) nos termos da cláusula onze – da liquidação e pagamento;

c) observar e cumprir, estritamente, os termos da proposta e as condições ora estabelecidas, obedecendo a critérios e prazos acordados pelas exigências técnicas constantes do edital e contrato;

d) manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

d.1) manter a regularidade fiscal e trabalhista durante todo o período contratual, sob pena de rescisão contratual e de execução da retenção sobre os créditos da empresa e/ou da eventual garantia, a título de multa, para ressarcimento dos valores e indenizações devidos à Administração, além das penalidades previstas em lei;

d.2) se for Optante pelo Simples Nacional deverá apresentar a Declaração, conforme modelo constante no Anexo IV da Instrução Normativa nº 1.234/2012 da Receita Federal do Brasil, no momento da apresentação da primeira nota fiscal/fatura decorrente da assinatura do contrato ou da prorrogação contratual;

d.3) informar imediatamente qualquer alteração da sua permanência no Simples Nacional;

e) responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais, resultantes da execução do contrato, *ex vi* do *caput* do art. 121 da Lei nº 14.133/2021;

f) reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados (art. 119 da Lei 14.133/2021);

g) manter quadro de pessoal suficiente para atendimento dos serviços, conforme previsto neste contrato e em legislação específica, sem interrupção, seja por motivo de férias, descanso semanal, licença, greve, falta ao serviço e demissão de empregados, que não terão em hipótese alguma, qualquer relação de emprego com o Contratante;

h) prestar todos os esclarecimentos que forem solicitados pelos responsáveis pelo acompanhamento e fiscalização da execução do contrato;

i) fornecer crachás para seus empregados, sendo obrigatório seu uso nas dependências do Contratante;

j) substituir imediatamente qualquer um de seus empregados que for considerado inconveniente à boa ordem e às normas disciplinares do Contratante;

k) responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo, quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Contratante;

l) durante toda a execução do contrato, manter-se, em conformidade com as obrigações assumidas, atendendo a todas as condições de habilitação e qualificação exigidas na licitação;

m) atentar para as práticas de sustentabilidade na execução dos serviços nos termos do art. 6º do Capítulo III da Instrução Normativa nº 01, de 19/01/2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão;

n) obedecer, no que couber, aos princípios e normas de condutas estabelecidas no Código de Ética do Contratante;

o) arcar com despesa decorrente de qualquer infração, seja de que natureza for, desde que praticada por seus empregados no recinto do Contratante;

p) informar e manter atualizado endereço de *e-mail* válido, para comunicação oficial entre Contratante e Contratada;

q) a Contratada deverá, em até 10 dias após a comunicação da assinatura do contrato, indicar empregado para exercer o papel de Preposto, bem como seu *e-mail* e telefone de contato. O Preposto deve ter capacidade gerencial para tratar todos os assuntos previstos neste Termo de Referência e no instrumento contratual correspondente, sem implicar em ônus para o Contratante;

r) caso ocorra a inexecução total do contrato pela Contratada, sem prejuízo das multas e demais sanções previstas em lei, fica estabelecido que a Contratada deverá restituir integralmente o valor pago antecipadamente pelo Contratante. O valor a ser restituído deverá

ser atualizado monetariamente com base no Índice de Custos de Tecnologia da Informação (ICTI), estabelecido na Portaria nº 6.432, de 11 de julho de 201829, do Ministério do Planejamento, Desenvolvimento e Gestão (ou outro índice definido pela Equipe de Planejamento da Contratação durante a elaboração deste Termo de Referência). A atualização monetária será aplicada desde a data do pagamento antecipado até a data da efetiva restituição;

s) caso ocorra a inexecução parcial do contrato pela Contratada, sem prejuízo das multas e demais sanções previstas em lei, fica estabelecido que a Contratada deverá realizar a restituição proporcional dos valores pagos antecipadamente pelo Contratante;

t) a restituição proporcional será calculada com base na porcentagem de execução dos serviços previstos no contrato. O valor a ser restituído será atualizado monetariamente com base no Índice de Custos de Tecnologia da Informação (ICTI), estabelecido na Portaria nº 6.432, de 11 de julho de 2018, do Ministério do Planejamento, Desenvolvimento e Gestão (ou outro índice definido pela EPC durante a elaboração deste Termo de Referência). A atualização monetária será aplicada desde a data do pagamento antecipado até a data da efetiva restituição;

u) o local de prestação dos serviços constará no Anexo II.

§ 2º – Das obrigações da Contratada em face da LGPD:

a) para os fins da Lei Geral de Proteção de Dados (Lei n. 13.709/18), na hipótese de, em razão do presente contrato, a Contratada realizar o tratamento de dados pessoais como operadora ou controladora, deverá adotar as medidas de segurança técnicas, jurídicas e administrativas aptas a proteger tais dados pessoais de acessos não autorizados ou qualquer forma de tratamento inadequado ou ilícito, observando-se os padrões mínimos definidos pela Autoridade Nacional de Proteção de Dados em conformidade com o disposto na legislação de proteção de dados e privacidade em vigor, sem prejuízo do disposto nas alíneas subsequentes;

b) dar tratamento aos dados pessoais a que tiver acesso por força do contrato tão-somente na medida do cumprimento do escopo contratual, vedado o tratamento para quaisquer outros propósitos;

c) não fornecer transferir ou disponibilizar dados pessoais a terceiros, a menos que com base em instruções explícitas, por escrito, do Contratante ou por ordem de autoridade judicial, sob a condição de que, nesse último caso, informando ao Contratante dentro de 24 (vinte e quatro) horas após o recebimento da ordem judicial, ressalvadas as hipóteses legais de sigilo na investigação em que o tratamento sigiloso tenha sido expressamente exigido pela autoridade judicial, quando a Contratada estará dispensada da comunicação ao Contratante;

d) não colocar o Contratante em situação de violação da LGPD;

e) assegurar que seus empregados tenham ciência dos termos da LGPD, que assinem o “Termo de Confidencialidade e de Responsabilidade”, e que estejam capacitados para agir dentro das normas nela dispostas;

f) assegurar que as pessoas autorizadas a tratar os dados pessoais assinem o “Termo de Confidencialidade e de Responsabilidade”;

g) responsabilizar-se pelo uso indevido que seus empregados ou prestadores de serviços fizerem dos dados pessoais a que tiverem acesso pela execução contratual, bem como por quaisquer falhas nos sistemas por ela empregados para o tratamento dos dados;

h) cessar o tratamento de dados pessoais realizado com base no Contrato imediatamente após o seu término e, a critério exclusivo do Contratante, apagar, destruir ou devolver os dados pessoais que tiver obtido;

i) nos casos em que realizar o tratamento de dados pessoais confiados pelo Contratante, a Contratada será considerada "operadora" e deverá aderir à Política de Privacidade e Proteção de Dados do Contratante.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DO CONTRATANTE

O Contratante se obriga a:

a) acompanhar a execução do contrato, nos termos do art. 117 da Lei nº 14.133/21, através dos responsáveis pelo acompanhamento e fiscalização da execução do contrato, que exercerá ampla e irrestrita fiscalização do objeto do presente contrato, a qualquer hora, determinando o que for necessário à regularização das faltas ou defeitos observados, inclusive quanto às obrigações da Contratada;

b) proporcionar todas as facilidades necessárias à boa execução deste contrato, especialmente as condições indispensáveis para o acesso seguro ao ambiente;

c) efetuar os pagamentos devidos à Contratada, nos prazos e condições ora estabelecidos;

d) prestar as informações e esclarecimentos que venham a ser solicitados pela Contratada.

CLÁUSULA NONA – DA GESTÃO E FISCALIZAÇÃO DA EXECUÇÃO DO CONTRATO

Atuará como gestor deste Ajuste, nos termos da Instrução Normativa TRT nº 07/2013 e do art. 117 da Lei 14.133/2021, o Secretário de Infraestrutura Tecnológica ou seu substituto eventual.

§1º - A execução deste Ajuste deverá ser acompanhada e fiscalizada pelos fiscais do Contrato, devendo observar o seguinte:

a) Atuarão como fiscais administrativo e técnico deste Contrato os servidores vinculados à Secretaria de Infraestrutura Tecnológica ou seus substitutos eventuais, também vinculados à Seção citada (Lei n. 14.133/2021, art. 117, *caput*).

I - Atribuições do gestor do contrato:

a) gerir a execução do ajuste;

b) acompanhar as ações de fiscalização;

c) diligenciar junto à empresa nos casos em que lhe forem solicitados pelo fiscal;

d) realizar o recebimento definitivo e,

e) ao final do contrato, emitir o Termo de Encerramento de Contrato.

II - Atribuições dos fiscais do contrato:

a) inteirar-se dos termos do contrato, gerenciar minuciosamente o cumprimento dos níveis de serviço e atentar para os prazos contratuais (prazo de início de serviço, prazo para entrega do material, para a execução do serviço etc.);

b) promover as ações necessárias para regularização das faltas ou defeitos observados na execução contratual, com objetivo de que ocorra nos termos acordados;

c) eventuais decisões e providências que ultrapassem suas competências deverão ser solicitadas ao gestor em tempo hábil para a adoção das medidas convenientes.

III - Atribuições do fiscal administrativo:

a) deverá realizar, mensalmente, os seguintes exames, que deverão estar anotados no Termo de Conformidade para Pagamento da Nota Fiscal:

i. comprovante de regularidade fiscal, constatada via consulta “on-line” ao Sistema de Cadastramento Unificado de Fornecedores (SICAF) e no Cadastro de Empresas Inidôneas e Suspensas - CEIS;

ii. verificar se as condições de pagamento do contrato foram obedecidas e o valor cobrado corresponde àquilo que foi fornecido (de acordo com as informações do Termo de Recebimento Provisório e medição dos Níveis Mínimos de Serviços);

b) quanto ao recebimento dos bens adquiridos, o fiscal administrativo deve verificar a regularidade fiscal da contratada e a observância dos prazos para entrega dos bens;

IV - Atribuições do fiscal demandante:

a) verificar se a execução do contrato obedece aos critérios funcionais estabelecidos, devendo apresentar manifestação no processo da contratação sempre que entender necessário, para eventual correção de inconsistências verificadas.

V - Atribuições do fiscal técnico:

a) realizar verificação dos seguintes aspectos:

i. os resultados alcançados em relação ao contrato, com a verificação do prazo de execução da qualidade demandada;

ii. qualidade e quantidade dos recursos utilizados;

iii. adequação dos serviços prestados à rotina de execução estabelecida;

iv. adequação do bem entregue às especificações estabelecidas;

b) realizar o de recebimento provisório.

§ 1º – O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do contrato.

§ 2º – A fiscalização exercida pelo Contratante não excluirá ou reduzirá a responsabilidade da Contratada pela completa e perfeita execução do objeto contratual, tampouco restringe a responsabilidade integral e exclusiva da Contratada quanto à integralidade e à correção dos fornecimentos a que se obrigou, suas consequências e implicações perante terceiros, próximas ou remotas.

§ 3º – A Contratada declara aceitar, integralmente, todos os métodos e processos de inspeção, verificação e controle a serem adotados pelo Contratante.

CLÁUSULA DEZ – DO PREÇO

O valor do presente contrato é de **R$ 3.901.534,00 (Três milhões, novecentos e um mil, quinhentos e trinta e quatro reais)**, assim discriminado:

Item	Descrição	Unidade	Valor (R$)
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7, por 60 meses adicionais, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewall*, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	*Cluster*	**3.901.534,00**

Parágrafo único – Estão incluídas no preço todas as despesas relativas à consecução eficiente e integral do objeto deste contrato.

CLÁUSULA ONZE – DA LIQUIDAÇÃO E DO PAGAMENTO

A liquidação e o pagamento serão assim efetuados:

a) os pagamentos serão realizados na forma do SIGEO JT – Sistema Integrado de Gestão Orçamentária e Financeira da Justiça do Trabalho – Módulo Execução Orçamentária.

b) para fins de liquidação e pagamento, é de exclusiva responsabilidade da Contratada o seu cadastramento no SIGEO, gestão de seus dados e a juntada por meio do referido Sistema dos documentos de cobrança/documentos fiscais (notas fiscais/faturas);

c) é de exclusiva responsabilidade da Contratada as ações indicadas na alínea anterior não cabendo ao Contratante qualquer responsabilidade pela falta de juntada ao sistema no prazo;

d) eventuais dúvidas poderão ser dirimidas junto à Secretaria de Infraestrutura Tecnológica, por meio do *e-mail* seit@trt3.jus.br ou telefone (31) 3238-7902;

e) a nota fiscal deverá ser juntada, pela Contratada, no sistema SIGEO-JT Execução Financeira e os documentos exigidos na contratação deverão ser encaminhados ao *e-mail* seit@trt3.jus.br;

f) a equipe de gestão e fiscalização deverá proceder o recebimento provisório e definitivo do objeto, em conformidade com a Instrução Normativa TRT3 n. 07/2013.

g) o prazo para pagamento é de 10 (dez) dias úteis a contar da apresentação da fatura acompanhada do respectivo recebimento definitivo do objeto e conforme a tabela abaixo, que especifica a periodicidade do pagamento:

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG Firewall utilizada na JT		
Item	**Descrição**	**Periodicidade**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7, por 60 meses adicionais, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewall*, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento único e antecipado - Pagamento em parcela única, antecipada.**	Único

g.1) o item 1 possui pagamento antecipado, pois esta condição é o padrão de mercado e quanto pelos contratos atuais de outros órgãos;

h) para todos os fins, considera-se como data de pagamento, o dia da emissão da ordem bancária;

i) os pagamentos serão realizados de acordo com o cronograma de desembolso do Governo Federal, em moeda corrente nacional, sendo efetuada a retenção na fonte dos tributos e contribuições elencados nas disposições determinadas pelos órgãos fiscais e fazendários em conformidade com as instruções normativas vigentes;

j) havendo erro na (s) nota (s) fiscal (is)/fatura (s) ou qualquer circunstância que impeça a liquidação da despesa, aquela será restituída ou será comunicada a irregularidade à Contratada, ficando pendente de pagamento até que esta providencie as medidas saneadoras. Nesta hipótese, o prazo para o pagamento iniciar-se-á após a regularização da situação e/ou a reapresentação do documento fiscal, não acarretando qualquer ônus para o Contratante;

k) a Contratada será a responsável direta pelo faturamento a que se propõe, não podendo ser aceito documento de cobrança (nota fiscal/fatura) emitido por empresa com a raiz do Cadastro Nacional de Pessoa Jurídica – CNPJ diferente ao daquela, ainda que do mesmo grupo empresarial;

k.1) as Unidades responsáveis pela execução do objeto contratual e detentoras de numeração da raiz do CNPJ idêntica à da Contratada, divergindo somente o sufixo e dígito verificador, poderão emitir Nota Fiscal/Fatura, desde que satisfaçam as condições de habilitação e a regularidade fiscal exigida no processo;

l) a Contratada deverá apresentar, sempre que solicitado pelo Contratante, as certidões abaixo discriminadas:

- CRF – Certificado de Regularidade do FGTS, emitido pela CEF;
- Certidão Negativa de Débitos Relativos aos Tributos Federais e à Dívida Ativa da União, emitida em conjunto pela Secretaria da Receita Federal e

Procuradoria-Geral da Fazenda Nacional;

- CNDT - Certidão Negativa de Débitos Trabalhistas, emitida pela Justiça do Trabalho;
- Prova de regularidade para com a Fazenda Estadual do seu domicílio ou de sua sede;
- Prova de regularidade para com a Fazenda Municipal do seu domicílio ou de sua sede;

m) o Contratante poderá reter o pagamento dos valores referentes ao fornecimento realizado nas hipóteses da cláusula catorze, limitado ao valor do dano, ressalvada a possibilidade de rescisão contratual;

n) o Contratante poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela Contratada, nos termos deste contrato;

o) no ato do pagamento será retido na fonte o Imposto sobre a Renda de Pessoa Jurídica, a contribuição sobre o lucro, a contribuição para a seguridade social (CONFINS) e a contribuição para O PIS/PASEP, todos da Secretaria da Receita Federal. No entanto, não recairá esta retenção sobre pessoas jurídicas que apresentarem a Declaração de Optante do Simples, conforme modelo constante no Anexo IV da Instrução Normativa nº. 1.234/2012 da Receita Federal ou cópia da Consulta ao Portal do Simples Nacional da apresentação da primeira nota fiscal/fatura decorrente de assinatura contratual e de prorrogação contratual;

p) se os valores do pagamento forem insuficientes para a quitação das eventuais multas, fica a Contratada obrigada a recolher a importância devida, via GRU, no prazo de até 10 (dez) dias contados da comunicação oficial, sob pena de ser incluído o valor na Dívida Ativa da União.

CLÁUSULA DOZE – DO REAJUSTE

Os preços constantes do contrato serão reajustados, respeitada a periodicidade mínima de um ano a contar da data do orçamento estimado ou da data do último reajuste, limitado o reajuste à variação do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA ou de outro índice que passe a substituí-lo, e na falta deste, em caráter excepcional, será admitida a adoção de índices gerais de preços de acordo com a seguinte fórmula:

$$R = \frac{I - Io}{Io} \times P$$ **onde:**

a) para o primeiro reajuste:

R = reajuste procurado;

I = índice relativo ao mês de reajuste;

Io = índice relativo ao mês da data limite para apresentação da proposta;

P = preço atual dos serviços/contrato;

b) para os demais reajustes:

R = reajuste procurado;

I = índice relativo ao mês do novo reajuste;

Io = índice relativo ao mês do último reajuste efetuado;

P = preço do serviços/contrato atualizado até o último reajuste efetuado.

§ 1º – Em caso de ocorrência de deflação ou qualquer outro evento que possa implicar redução do valor contratual para adequá-lo aos preços de mercado, será provocada pelo Contratante mediante a apresentação de planilha com demonstração analítica da variação dos componentes dos custos do contrato no período correspondente, com vistas à definição do novo valor contratual a ser aplicado.

§ 2º – O valor e a data do reajuste serão informados no contrato mediante apostila.

CLÁUSULA TREZE – DA DOTAÇÃO ORÇAMENTÁRIA

As despesas com o presente contrato correrão à conta dos recursos orçamentários próprios, por meio da verba PTRES 168031-339040 e Nota de Empenho 2026NE36, emitida em 19/01/2026 pelo Contratante.

CLÁUSULA CATORZE – DA RESPONSABILIDADE CIVIL

A Contratada será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante, *ex vi* do art. 120 da Lei nº 14.133/21.

CLÁUSULA QUINZE – DAS SANÇÕES ADMINISTRATIVAS

Pela inexecução total ou parcial do contrato, a Administração poderá, garantida a ampla defesa, aplicar à Contratada as seguintes sanções:

I – Advertência, que será aplicada nas infrações contratuais leves, que não justifiquem a aplicação de penalidade mais rigorosa.

II – Multa, nos termos do inc. II do art. 156 da Lei 14.133/21, a ser aplicada a qualquer das infrações administrativas previstas no art. 155 da Lei 14.133/21:

a) multa moratória, pela infração administrativa prevista no inc. VII do art. 155 da Lei nº 14.133/21: decorrente de inobservância dos prazos para cumprimento de obrigações contratuais, na forma definida no edital e no contrato, arbitrada em 0,3% (três décimos por cento) por dia sobre o valor do(s) item(s) em mora, limitada a 10%;

a.1) se o atraso for superior a 30 (trinta) dias, poderão ser aplicadas cumulativamente as penas de multa moratória e compensatória, facultando-se, ainda, promover a rescisão contratual;

a.2) não sendo possível quantificar o valor da multa moratória ou se ele se mostrar incompatível com o disposto no art. 2º, parágrafo único, inciso VI, da Lei nº 9.784/99, a multa será de R$ 1.000,00, podendo este valor ser aplicado em dobro, se as circunstâncias do caso concreto assim recomendarem;

b) multa compensatória, a ser aplicada pelo cometimento de qualquer das infrações previstas no art. 155 da Lei nº 14.133/2021, na forma definida no edital, no contrato:

b.1) multa por inexecução parcial arbitrada em 10% (dez por cento) do item/valor mensal do contrato, e aplicada em dobro no caso de reincidência, por ocorrência das infrações administrativas previstas nos incisos I e II do art. 155 da Lei nº 14.133/21;

b.2) multa por inexecução total arbitrada em 10% (dez por cento) do valor total do contrato e aplicada por ocorrência da infração administrativa prevista no inc. III do art. 155 da Lei nº 14.133/21;

b.3) multa arbitrada em 10% (dez por cento) sobre o valor total do contrato, e aplicada em dobro no caso de reincidência, por ocorrência das infrações administrativas previstas nos inc. IV a XII do art. 155 da Lei nº 14.133/01;

b.4) multa de 1% (um por cento) sobre o valor da nota fiscal, a ser aplicada a cada ocorrência de violação da obrigação da manutenção da regularidade fiscal e trabalhista, durante toda a execução do contrato.

III – Impedimento de licitar e contratar com a União, nos termos do inc. III do art. 156 da Lei nº 14.133/21, pelo prazo máximo de até 3 (três) anos, que será aplicada por ocorrência das infrações administrativas previstas nos incisos II a VII do caput do art. 155 da Lei 14.133/21, quando não se justificar a imposição de penalidade mais grave.

IV – Declaração de inidoneidade para licitar ou contratar com a Administração Pública, nos termos do inc. IV do art. 156 da Lei nº 14.133/21, que será aplicada por ocorrência das infrações administrativas previstas nos incisos VIII a XII do caput do art. 155 da Lei nº 14.133/21, bem como pelas infrações administrativas previstas nos incisos II a VII do caput do referido artigo que justifiquem a imposição de penalidade mais grave que a sanção de impedimento, referida na alínea “c” deste parágrafo, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

V – As sanções previstas nos incisos I, III e IV poderão ser aplicadas cumulativamente com a prevista no inciso II deste parágrafo.

§ 1º – Penalidades da Contratada em face da LGPD:

O descumprimento das obrigações relativas ao tratamento de dados previstas na cláusula sétima incidirá nas seguintes penalidades:

a) até 10% (dez por cento) sobre o valor mensal do contrato, na hipótese de utilização dos dados pessoais para finalidade diversa daquela estabelecida para a execução contratual;

b) até 20% (vinte por cento) sobre o valor mensal do contrato, na hipótese de do compartilhamento não autorizado de dados pessoais com terceiros.

I – As penalidades previstas nas alíneas “a” e “b” serão aplicadas por ocorrência e, no caso de reincidência, serão aplicadas em dobro.

II – As penalidades previstas nas alíneas “a” e “b” não excluem a responsabilidade das empresas pela aplicação das sanções previstas no art. 52 e o ressarcimento de danos, na forma prevista no § 4º do art. 42, ambos da LGPD.

§ 2º – Na aplicação das penalidades previstas nesta cláusula, serão observados os conceitos, critérios, prazos e procedimentos estabelecidos pelo Contratante.

§ 3º - Caso os prazos estabelecidos para garantia sejam extrapolados e não seja apresentada, ou não seja aceita justificativa para tal atraso, serão aplicadas multas conforme tabela abaixo:

Atraso na prestação da Garantia	1ª Ocorrência (% do valor do contrato)	Reincidência (1) (% do valor do contrato)
1 a 5 dias	1%	2%
6 a 10 dias	2%	4%
11 ou mais dias	3%	6%

(1) A reincidência fica configurada a partir do segundo atraso registrado no atendimento destes serviços, mesmo que tratem de equipamentos distintos.

CLÁUSULA DEZESSEIS – DA EXTINÇÃO DO CONTRATO

Nos termos do art. 137, da Lei nº 14.133/21, constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, às seguintes situações:

I – Não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos.

II – Desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior.

III – Alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato.

IV – Decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado.

V – Caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato.

VI – Atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto.

VII – Atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas.

VIII – Razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade contratante.

IX – Não cumprimento das obrigações relativas à reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz.

§ 1º – A extinção do contrato poderá ser:

I – Determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta.

II – Consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração.

§ 2º – O descumprimento reiterado da obrigação da apresentação das certidões elencadas na alínea "l" da cláusula onze e a manutenção em situação irregular perante as obrigações fiscais e trabalhistas poderão dar ensejo à extinção contratual, respeitada a ampla defesa, em face de configurada a inexecução do contrato e a ofensa à regra trazida no art. 92, inciso XVI, da Lei nº 14.133/2021.

CLÁUSULA DEZESSETE – DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO AO EDITAL E À PROPOSTA

I – O presente contrato fundamenta-se:

- na Lei nº 14.133/21;
- na Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais);
- do § 5º, do art. 12, da Resolução CNJ nº 468/2022;
- nos preceitos de direito público e, supletivamente, os princípios da teoria geral dos contratos e as disposições de direito privado, nos termos do caput do art. 89 da Lei nº 14.133/21.

II – E vincula-se aos termos:

- do edital do processo nº PE 11636/2025, conforme § 2º do art. 89 da Lei nº 14.133/21;
- da proposta da Contratada, conforme § 2º do art. 89 da Lei nº 14.133/21;
- da ata de registro de preços;
- da Resolução GP nº 212/2021 do Contratante – Política de Privacidade e Proteção de Dados Pessoais;
- do Código de Ética do Contratante.

CLÁUSULA DEZOITO – DA ALTERAÇÃO DO CONTRATO

O disposto neste contrato somente poderá ser alterado pelas partes por meio de termos aditivos, asseguradas as prerrogativas conferidas à Administração, enumeradas no caput do art. 104 da Lei nº 14133/2021 e na cláusula sexta, mediante a apresentação das devidas justificativas e autorização prévia da autoridade competente, assegurados os direitos da Contratada de que tratam os §§ 1º e 2º do art. 58 da mesma Lei.

Parágrafo único – Nos termos do que dispõe o art. 125 da Lei nº 14.133/21, a Contratada fica obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários em até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA DEZENOVE – DAS DISPOSIÇÕES FINAIS

Além das disposições trazidas no presente contrato, aplicam-se, ainda, o seguinte:

a) a prestação de serviços, objeto do presente contrato, não gera vínculo empregatício entre os empregados da Contratada e a Administração, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta;

b) nada no presente contrato poderá ser interpretado como a criar quaisquer vínculos trabalhistas entre empregados da Contratada e o Contratante. A Contratada assume toda a responsabilidade por todos os encargos trabalhistas decorrentes da prestação de serviços por seus empregados;

c) a tolerância de uma parte para com a outra quanto ao descumprimento de qualquer uma das obrigações assumidas neste contrato não implicará novação ou renúncia de direito. A parte tolerante poderá exigir da outra o fiel e cabal cumprimento deste contrato a qualquer tempo;

d) as obrigações contidas nas cláusulas sétima e oitava não são de natureza exaustiva, podendo constar no presente termo obrigações referentes às partes ou a cada parte, que não estejam incluídas no rol de obrigações acima citadas;

e) os termos e disposições constantes deste contrato prevalecerão sobre quaisquer outros entendimentos ou acordos anteriores entre as partes, expressos ou implícitos referentes às condições nele estabelecidas;

f) é vedado à Contratada caucionar ou utilizar o presente contrato para qualquer operação financeira;

g) a Contratada se compromete a guardar sigilo absoluto sobre as atividades decorrentes da execução dos serviços e sobre as informações a que venha a ter acesso por força da execução dos serviços objeto deste contrato;

h) dos atos da Administração decorrentes da aplicação da Lei nº 14.133/21 cabe recurso e pedido de reconsideração, no prazo de 3 (três) dias úteis contados da intimação, nos termos do art. 165;

i) os casos omissos serão dirimidos pela Administração, que poderá disponibilizar em meio eletrônico informações adicionais e expedir normas complementares, em especial sobre as sistemáticas de fiscalização contratual;

j) o princípio da legalidade impõe à Administração a obrigação de fundamentar todos os seus atos, contratos e condutas no ordenamento jurídico. Por decorrência lógica, o tratamento dos dados pessoais coletados pelo Tribunal no presente Contrato para viabilizar sua formalização está em integral conformidade com a Lei nº 13.709/2019 (Lei Geral de Proteção de Dados – LGPD). Nesse sentido, observa a boa-fé e os princípios elencados no art. 6º, especialmente em relação à proteção dos dados e finalidades de sua utilização. O tratamento desses dados prescinde de consentimento do titular (art. 7º, III), inclusive para eventual compartilhamento (art. 26, § 1º, IV, c/c art. 27, III), e terão sua publicidade de acordo com as exigências legais.

CLÁUSULA VINTE – DA DIVULGAÇÃO NO PNCP

O Contratante é responsável pela divulgação do contrato no Portal Nacional de Contratações Públicas (PNCP), nos termos e prazos previstos no art. 94 da Lei nº 14.133/21.

CLÁUSULA VINTE E UM – DO FORO

As questões decorrentes da execução deste contrato, que não puderem ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de Belo Horizonte - MG, com exclusão de qualquer outro, por mais privilegiado que seja.

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

Belo Horizonte, data da última assinatura.

PATRICIA HELENA DOS REIS:30833897
Assinado de forma digital por PATRICIA HELENA DOS REIS:30833897
Dados: 2026.01.22 12:39:37 -03'00'

TRIBUNAL REGIONAL DO TRABALHO DA TERCEIRA REGIÃO
Patrícia Helena dos Reis
Diretora-Geral

PATRICIA ANGELINA DA CONCEICAO:34699483801
Assinado de forma digital por PATRICIA ANGELINA DA CONCEICAO:34699483801
Dados: 2026.01.19 16:13:55 -03'00'

NTSEC - SOLUÇÕES EM TELEINFORMÁTICA LTDA.
Patrícia Angelina da Conceição
Sócia Administradora

ANEXO I - Especificações Técnicas para Solução de Next Generation Firewall - NGFW

Inicialmente, apresenta-se na tabela A1 a lista de produtos previstos para aquisição como solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall.

Tabela A1 - Produtos a serem adquiridos

Grupo I - Contratação do serviço de suporte e manutenção para solução de NG *Firewall* utilizado na JT		
Item	**Descrição**	**Unidade (1)**
1	Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7, por 60 meses adicionais, para solução de proteção de perímetro de rede lógica do tipo *Next Generation Firewall*, com alta disponibilidade, incluindo software de administração e gerência integrada - **Tipo I - Pagamento em parcela única, antecipada.**	Cluster

(1) Ver definição de cluster abaixo.

Definições importantes:

Cluster: conjunto de dois, ou mais, equipamentos appliances compatíveis entre si, que trabalham de forma integrada e foram construídos especificamente para exercer a função de Next Generation Firewall.

Garantia de funcionamento: todos os serviços e atividades necessários para manter a solução em perfeito estado de funcionamento e que não envolvam operação ou configuração, tais como: manutenção corretiva, substituição de peças e componentes, substituição de equipamentos, atualizações de versões de hardware e software, revisões e/ou distribuições (releases) e correções (patches) dos programas (softwares, firmwares, drivers), etc. Deve incluir ainda o acesso, por meio da Internet, de base de documentos e conhecimentos mantida pela fabricante da solução, contemplando seus manuais de instalação. (responsabilidade do fabricante)

Atualização de assinaturas de proteção: acesso e meios para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por botnets, listas de endereços IPs de reputação duvidosa, etc. (responsabilidade do fabricante)

Suporte técnico: todos os serviços e atividades necessários à detecção de problemas de configuração e diagnóstico acerca de vícios e problemas dos produtos a fim de proporcionar o uso adequado e otimizado da solução, incluindo o esclarecimento de dúvidas, sugestão de melhores práticas e orientação técnica da Equipe Técnica do contratante.

A tabela A2 apresenta um compêndio dos prazos previstos na contratação.

Tabela A2 - Prazos da contratação

Item	Descrição da Atividade	Prazo
1	Início do Serviço de garantia e atualização de assinaturas de proteção e suporte técnico	Até 10 dias após a comunicação da assinatura do contrato.

Antes de iniciar a descrição dos requisitos detalhados para a solução, como a solução de NG Firewall e SASE são complexos, implicam em risco de interrupção da prestação jurisdicional e ainda, em caso de substituição de fornecedor, é necessário obter nova quantidade profissionais terceiros e dos Tribunais para assegurar a continuidade da prestação, a EPC entende que, independente dos demais requisitos, o prazo de vigência de 60 meses é o mais adequado. Este período propiciará uma segurança para as equipes de TIC dos Tribunais, e também permitirá que as empresas amortizem seus investimentos em profissionais qualificados, garantindo maior concorrência, como também preços mais vantajosos considerando os custos de mobilização e desmobilização. Esse prazo também garante que a prestação jurisdicional não sofrerá pela troca de solução de Firewall, no mínimo, por 5 anos.

1. Requisitos para a Solução de NGFW - Grupo I, Item I - Contratação do serviço de suporte e manutenção para solução de NG Firewall

Esta seção trata de especificações para os equipamentos que compõem a Solução de alta disponibilidade de Next Generation Firewall, licenças e periféricos necessários para o seu pleno funcionamento nos ambientes on premises do Órgão Público participante.

Como o Firewall é uma solução que identifica e protege, em tempo real, Redes e dispositivos do contratante, que estão submetidos a ataques constantemente renovados, este mecanismo fica comprometido quando desatualizado. Portanto, é imprescindível assegurar que a solução de Firewall esteja sempre em sua versão mais recente.

O Item I do Grupo I contempla a renovação do serviço de garantia, atualização de assinaturas de proteção e suporte técnico para os equipamentos que já estão em uso no Contratante.

1.1. Especificação dos Equipamentos do Grupo I item I - Tipo I

Os equipamentos Tipo I são os equipamentos que foram dimensionados pelo fabricante Checkpoint para substituir os equipamentos que já estavam em operação nos tribunais que participaram da contratação de extensão de garantia Processos Administrativos 3928/2023 e 9665/2023 e que tiveram seus equipamentos antigos declarados como end-of-life end-of-support durante a vigência do contrato.

O Equipamento Tipo I é o modelo Quantum 16200 Plus do fabricante Checkpoint.

No caso de troca de equipamentos, os novos equipamentos devem ter capacidade idêntica ou superior ao antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior, bem como as especificações do item 1.2 deste Anexo.

1.2. Características comuns para os equipamentos que compõem cada Cluster do Item I do Grupo I - Tipo I

Os equipamentos que compõem os Clusters do Item I do Grupo I da contratação deverão ser do mesmo fabricante (Checkpoint), conforme justificativa constante no ETP.

A seguir serão especificadas as características comuns para os equipamentos referentes ao Grupo I, Item I do Edital e Termo de Referência da presente contratação.

1.2.1. O hardware para cada equipamento appliance que compõem o cluster deve constar as seguintes características:

a) Deve ser apropriado para o uso em ambiente tropical, com umidade relativa entre 10 e 85% (sem condensação) e temperatura ambiente na faixa de 0°C a 40°C;
b) O fluxo do ar refrigerado deve ser recebido pela parte dianteira e dispensado na parte traseira do equipamento;
c) Possuir 2 (duas) fontes de alimentação independentes, redundantes e com capacidade de substituição sem desligar o equipamento (hot-swappable), com alimentação nominal de 100~120VAC e 210~230VAC, frequência de funcionamento de 50 ou 60Hz, ou ainda com ajuste automático de tensão e frequência (auto-ranging), por appliance;
d) Deverá vir acompanhado de cabos de alimentação para todas as fontes, com, no mínimo, 1,80m, com plugue tripolar 2P+T no padrão ABNT NBR 14136;
e) Deverá 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);
f) Possuir no mínimo 1 (uma) porta de console para configuração e gerenciamento por interface de linha de comando (CLI);
g) Possuir, no mínimo, 1 (uma) interface out-of-band dedicada para gerenciamento com capacidade compatível com o tipo do equipamento (I);
h) Possuir, no mínimo, 1 (uma) interface para o sincronismo de estados da solução de alta disponibilidade;
i) A interface de sincronismo não precisa, necessariamente, estar rotulada para a finalidade de sincronismo do recurso de alta disponibilidade, sendo aceitável qualquer interface do equipamento. A capacidade da interface deve ser compatível com cada tipo do equipamento (I);
j) Os equipamentos devem ser fornecidos em sua capacidade máxima de processamento e memória;
k) Possuir, no máximo, 4Us de altura;
l) Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, sem custos adicionais;
m) Possuir certificação de conformidade sustentável de acordo com os padrões EPA (Enviromental Protection Agency) ou similares, tais como EnergyStar, RoHS (Restriction on Hazardous Substances), WEEE (Waste Electrical and Electronic Equipment) ou EMI Certifications FCC part 15, CE, EN55022, EN55024;
n) Possuir certificação de conformidade da ANATEL ou serem fabricados no Brasil;
o) Deve informar, no painel de gerência do equipamento, a utilização dos recursos de CPU, memória, armazenamento interno e atividade de rede, podendo ser mostrado também no sistema de gerência centralizado, e;
p) Deve informar, no painel de gerência do equipamento, o número de conexões simultâneas e de novas conexões por segundo do equipamento, podendo ser mostrado também no sistema de gerência centralizado.

1.2.2. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale.

1.2.3. Cada equipamento (appliance) deve oferecer, no mínimo, as seguintes funcionalidades:

a) Suportar os protocolos IPv4 e IPv6;
b) Suportar, no mínimo, 1.024 VLANs no padrão IEEE802.1q;
c) Suportar agregação de links no padrão IEEE802.3ad;
d) Suportar o protocolo DHCP;
e) Suportar o protocolo NTP;

f) Suportar as funcionalidades de roteamento estático e dinâmico, em IPv4 e IPv6;
g) Suportar os protocolos RIP, OSPF v2, OSPF v3, BGP v4 (RFC 4271) e BGP v6;
h) Suportar os protocolos IGMP v2, IGMP v3 e PIM-SM;
i) Suportar os protocolos SNMP v2c e SNMP v3;
j) Possuir Management Information Base (MIB) própria contemplando, no mínimo, indicadores de estado do hardware e de performance do equipamento;
k) Suportar Policy Based Routing (PBR), ou Policy Based Forwarding (PBF), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação;
l) Suportar o funcionamento nos modos sniffer (para inspeção de tráfego gerado por uma porta de rede espelhada), camada 2 de rede (layer-2), camada 3 de rede (layer-3), e suas combinações;
m) Permitir o acesso ao equipamento via CLI (console), SSH e interface web HTTPS;
n) Possuir funcionalidades de Backup/Restore de sua configuração e políticas de segurança;
o) Permitir o agendamento automático dos Backups, podendo ser realizado pela solução de gerenciamento;
p) Armazenar os Backups localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP e SCP, e;
q) Criptografar e autenticar a comunicação com a solução de gerenciamento centralizado.

1.2.4. Funcionalidades de identificação de usuários da solução (appliance):

a) Promover a integração com serviços de diretório LDAP, via serviço de diretórios OpenLDAP e Active Directory, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos e ameaças;
b) Deve identificar de forma transparente os usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS, e ainda, para LDAP será admissível o uso de agentes nas estações de trabalho e servidores;
c) Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, Active Directory, RADIUS e proxies internos;
d) Será permitido que a solução de gerenciamento centralizado possua um “appliance virtual” específico para atendimento às necessidades de identificação e autenticação de usuários;
e) Possuir portal de autenticação (Captive Portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory, servidores RADIUS;
f) O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;
g) Permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP via serviço de diretórios OpenLDAP e Active Directory;
h) Registrar a identificação do usuário em todos os logs de eventos de acesso e de ameaças gerados pelo equipamento;
i) Registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (batches) ou processos de correlação após a ocorrência do evento em questão, e;
j) Deve estar licenciado e permitir a identificação e autenticação de pelo menos 10.000 (dez mil) usuários simultâneos.

1.2.5. Funcionalidades de Firewall por equipamento (appliance)

a) Não deve possuir restrições ao número de máquinas ou usuários protegidos;
b) Suportar a implementação tanto em modo transparente (layer-2) quanto em modo gateway (layer-3);
c) Suportar inspeção Stateful de tráfegos IPv4 e IPv6;
d) Suportar controle de acesso para pelo menos 90 serviços e protocolos pré-definidos;
e) Suportar os protocolos para transmissão de áudio e vídeo H.323, SIP e MGCP;
f) Suportar os protocolos de Streaming com compressão RTCP, RTMP, RTSP e RTP;
g) Implementar mecanismo de conversão de endereços NAT (Network Address Translation), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT, dependendo da origem, destino ou porta);
h) Permitir transição entre endereços de redes IPv4 e IPv6, permitindo a comunicação entre dispositivos que usam esses protocolos diferentes, por meio de NAT N46 (que permite IPv4 acessar IPv6) e NAT64 (que permite IPv6 acessar IPv4).
i) Permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino;
j) Implementar mecanismo de proteção contra ataques de falsificação de endereços IP (anti-spoofing), tanto para IPv4 quanto para IPv6;
k) Implementar mecanismo de captura de pacotes;
l) Identificar os usuários para qualquer protocolo ou aplicação baseada em TCP/UDP, na forma da seção 1.2.4 - Funcionalidades de identificação de usuários da solução (appliance);
m) Suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6;
n) Suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período, e suas combinações;
o) Deve ser possível a aplicação de novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas, salvo as conexões atingidas pelas regras alteradas, e;
p) Possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: Endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, status dos flags “ACK”, “SYN” e “FIN” ou sinalizar nos logs que o Three-way-handshake não foi concluído com sucesso, ação sobre o pacote (permitido ou negado).
q) A solução deve ser capaz de exportar dados de fluxo de tráfego (flows) para ferramentas externas de monitoramento e análise, usando protocolos tais como IPFIX (IP Flow Information Export) ou sFlow ou Netflow;

1.2.6. Funcionalidades de geolocalização por equipamento (appliance):

a) Identificar os países de origem e destino de todas as conexões estabelecidas com a Internet através do equipamento;
b) Suportar a atualização automática das listas de geolocalização;
c) Aplicar as atualizações sem perda das conexões ativas;
d) Armazenar as listas de geolocalização no próprio equipamento;
e) Permitir a criação de políticas de segurança baseadas em geolocalização, permitindo também o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países;
f) Possibilitar a visualização dos países de origem e destino nos logs de eventos de acessos e ameaças;

1.2.7. Funcionalidades de controle de acesso à Internet por equipamento (appliance)

a) Prover o controle e a proteção de acesso à Internet por meio do reconhecimento das aplicações, independente de porta e protocolo, e da classificação de URLs;
b) Identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas;
c) Identificar se as aplicações estão utilizando sua porta default;
d) Identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS;
e) Identificar aplicações criptografadas usando SSL/TLS;
f) Identificar um mínimo de 5.000 (cinco 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;
g) Deve ser capaz de identificar, pelo menos, as seguintes aplicações: Torrent, TOR, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger ou Facebook Chat, Google+, Google Chat, Tinder, Instagram, Twitter (X), Linkedin, Dropbox, Google Drive, One Drive, Logmein, TeamViewer, MSRDP, VNC, Ultrasurf, Webex, Zoom;
h) Permitir a criação de assinaturas para identificação de aplicações proprietárias do órgão, sem a necessidade de ação ou intervenção do fabricante;
i) Suportar a atualização automática da base de assinaturas utilizada na identificação das aplicações;
j) Permitir aplicar as atualizações sem perda das conexões ativas e das assinaturas customizadas;
k) Armazenar preferencialmente a base de assinaturas no próprio equipamento, aceitando-se também na solução de gerenciamento centralizado;
l) Classificar as aplicações em categorias, tecnologia e fator de risco;
m) Identificar os usuários que estão utilizando as aplicações, na forma da seção 1.2.4 - Funcionalidades de identificação de usuários da solução (appliance);
n) Permitir o bloqueio de aplicações que não estejam utilizando suas portas default;
o) Suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;
p) Permitir a utilização ou bloqueio individualizado das aplicações, para determinados usuários ou grupo de usuários;
q) Permitir registrar todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado;
r) Permitir o controle de uso de banda de download ou upload utilizada pelas aplicações (traffic shaping) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. Os controles descritos poderão ser aplicados individualmente ou combinados, conforme a necessidade da contratante;
s) Deve ser capaz de efetuar a classificação de conteúdo de páginas web em HTTP e HTTPS, baseado em listas de categorias;
t) Possuir, no mínimo, 60 categorias de URLs, incluindo, mas não se limitando, às seguintes categorias ou suas semelhantes[1]: adult, chat, drugs, gambling, games, hacking, hate speech, remote proxies, social networks, streaming média, violence, weapons;
u) Permitir sobrescrever as categorias de uma URL que se considere indevidamente classificada;

[1] O nome das categorias está em língua inglesa porque trata-se de uma prática comum entre os fabricantes de solução Firewall.

v) Permitir a criação de categorias/listas customizadas;
w) Permitir a inclusão de URLs customizadas nas categorias já existentes ou previamente customizadas;
x) Suportar a atualização automática das listas de categorias, e aplicação das atualizações sem perda das conexões ativas e das URLs customizadas;
y) Armazenar as listas de categorias no próprio equipamento ou na solução de gerenciamento centralizado;
z) Deve identificar os usuários que estão acessando as páginas web na forma da seção 1.2.4 - Funcionalidades de identificação de usuários da solução (appliance);
aa) Suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, fator de risco, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo. As políticas descritas poderão ser implementadas individualmente ou combinados, conforme a necessidade da contratante;
bb) Alertar o usuário quando uma URL for bloqueada por meio da página de bloqueio que possa ser customizada no próprio equipamento, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada;
cc) Permitir o bloqueio e continuação da navegação web (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão “Continuar” ou a inclusão de usuário e senha, para possibilitar o usuário continuar acessando o site), e;
dd) Registrar todos os acessos autorizados ou bloqueados às páginas web, incluindo sua classificação e o usuário identificado;

1.2.8. Funcionalidades de prevenção de ameaças por equipamento (appliance):

a) Possuir, no mínimo, funcionalidades de IPS, Antivírus, Anti-Bot, Anti-Malware e Anti-Spyware;
b) Possuir, no mínimo, os seguintes mecanismos de detecção: assinaturas de vulnerabilidades e exploits, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, detecção baseada em comportamento, nível de severidade do ataque e nível de confiança de detecção do ataque;
c) Possuir proteção contra ataques de negação de serviço DoS e DDoS;
d) Possuir assinaturas para bloqueio de ataques “buffer overflow”;
e) Possuir mecanismo automático de captura de pacotes de eventos de IPS, para fins de “troubleshooting” e análise forense;
f) Deve ser capaz de inspecionar tráfego criptografado usando protocolo SSL/TLS;
g) Deve ser capaz de inspecionar integralmente todos os pacotes de dados, sem prejuízo na performance do equipamento, para a seção 1.1 de acordo com os datasheets dos equipamentos já em operação e até os limites indicados nas seções 1.2 e 1.3;
h) Possuir referência cruzada da base de assinaturas de detecção com os identificadores CVE (Common Vulnerabilities and Exposures);
i) Possibilitar a criação de assinaturas customizadas;
j) Identificar os usuários relacionados aos eventos de IPS na forma da seção 1.2.4 - Funcionalidades de identificação de usuários da solução (appliance);
k) Possibilitar a criação de políticas de segurança que emitam alertas, sem realizar bloqueios, ao detectar a ocorrência de um ataque específico, identificando sua origem ou destino com base em um endereço IP ou rede CIDR específicos;
l) Permitir a criação de políticas de segurança capazes de bloquear ataques específicos por meio de ações como DROP (descarte) e/ou RESET (reinicialização da conexão), com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;

m) Permitir a criação de exceções ou exclusões para a inspeção de uma determinada assinatura ou grupo de assinaturas, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;
n) Registrar todos os eventos de IPS, incluindo o usuário identificado;
o) Identificar e bloquear a comunicação com botnets;
p) Bloquear malwares e spywares;
q) Inspecionar e bloquear vírus, ao menos, nos seguintes tipos de tráfego: FTP, HTTP, HTTPS e SMTP;
r) Suportar proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
s) Suportar a inspeção de vírus em arquivos comprimidos utilizando algoritmo deflate, como o padrão zip, gzip, entre outros;
t) Suportar bloqueio de download de pelo menos 50 tipos de arquivos como, arquivos tipo Executáveis, PDF, DLLs, Arquivos de Código, MSI, doc, xls, ppt, entre outros;
u) Suportar a atualização automática das bases de assinaturas para prevenção de ameaças;
v) Suportar aplicação das atualizações de prevenção de ameaças sem reinicialização do equipamento e nem perda das conexões ativas que não sejam afetadas pelas atualizações;
w) Armazenar as bases de assinaturas de prevenção de ameaças no próprio equipamento ou na solução de gerenciamento centralizado;
x) Identificar os usuários relacionados aos eventos de bloqueio relacionados a prevenção de ameaças na forma da seção 1.2.4 - Funcionalidades de identificação de usuários da solução (appliance);
y) Permitir a criação de políticas de segurança que gerem alertas, sem realizar bloqueios, ao detectar a ocorrência de uma ameaça específica, com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos;
z) Permitir a criação de políticas de segurança que bloqueiem a ocorrência de ameaças específicas com base na origem ou destino definidos por um endereço IP ou rede CIDR específicos, e;
aa) Suportar notificações e alertas sobre ameaças via e-mail, SNMP traps e log de pacotes;

1.2.9. Características de QoS por equipamento (appliance):

a) Permitir o controle de tráfego com base nas aplicações com, no mínimo as ações: permitir, negar, agendar o uso, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou cada usuário;
b) 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);
c) Suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP e RTP;
d) Suportar a marcação de pacotes DiffServ;
e) Permitir o monitoramento do uso da priorização de tráfego que as aplicações fazem por bytes, sessões e por usuário.

1.2.10. Características de inspeção SSL/TLS por equipamento (appliance):

a) Identificar, descriptografar e analisar o tráfego SSL e TLS 1.2/1.3 tanto em conexões de entrada (Inbound) quanto de saída (Outbound);
b) Deve permitir a descriptografia da área útil do pacote de dados (payload) para fins de controle de acesso à Internet e proteção contra ameaças, e;

c) Permitir a diferenciação de conexões pessoais (Bancos, Shopping, etc.) e conexões não pessoais por meio de classificação automática.

1.2.11. Características de VPN por equipamento (appliance):

a) Deve disponibilizar **licenciamento** para VPN site-to-site, sem limite do número de usuários simultâneos e sem limite do uso de túneis;
b) Suportar VPN site-to-site em topologias Full Meshed (todos os gateways possuem links específicos para todos os demais gateways) e também Estrela (gateways satélites se comunicam somente com um único gateway central);
c) Suportar, pelo menos, criptografias AES-128, AES-256;
d) Suportar integridade de dados com SHA-1 e SHA-256;
e) Suportar o protocolo IKE, fases I e II;
f) Suportar os algoritmos RSA e pelo menos 4 dos grupos Diffie-Hellman groups 1, 2, 5, 14, 15, 16, 17, 18;
g) Suportar NAT-T (NAT Transversal);
h) Deve possuir cliente próprio para instalação nos dispositivos fixos e móveis dos usuários, sem custo adicional e sem limite do número de usuários, e;
i) O cliente de VPN client-to-site deve ser compatível, ou suportar, o cliente nativo de pelo menos os seguintes Sistemas Operacionais: Windows 10 e Windows 11, Apple IOS versão 15 ou superior, Android versão 14 ou superior, Mac OS e Linux.
j) Deve permitir conexão VPN client-to-site de forma Clientless, com autenticação via browser, para fechar a VPN através de um portal TLS;
k) Deve suportar atribuição de endereço IP e de DNS dos clientes remotos de VPN;
l) Suportar Autenticação em Dois Fatores (2FA) para todos os usuários de VPN, sendo uma autenticação via usuário e senha, validados por bases LDAP com uso de serviço de diretórios OpenLdap, Active Directory, e base de usuários interna do appliance. Já o segundo fator pode ser Token gerado por e-mail (obrigatoriamente) e também protocolo TOTP e Certificado digital, admite-se ainda que o segundo fator seja implementado com ferramenta de terceiros;
m) Em relação ao certificado digital do item anterior, deverá ser compatível com: certificado emitido por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, CA externa de terceiros, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao Active Directory, e certificados emitidos por autoridade certificadora no padrão ICP-Brasil;
n) O túnel VPN do cliente ao gateway (client-to-site) deve fornecer uma solução de autenticação única (single-sign-on) aos usuários, integrando-se, no mínimo, com as ferramentas de Windows login da empresa Microsoft;
o) Permitir criação de políticas para usuários e grupos para tráfego de VPN client-to-site;
p) Integrar com serviços diretórios LDAP, via OpenLDAP e Active Directory, para a autenticação de usuários de VPN e também definição de regras de acesso;
q) Permitir a definição de condições específicas para autorizar o acesso remoto às redes internas via VPN client-to-site, garantindo maior segurança e controle. Entre essas condições, é necessário, no mínimo, suportar a verificação das versões dos Sistemas Operacionais dos dispositivos dos usuários, a exigência de um software antivírus instalado, ativo e com as definições atualizadas, e a validação das últimas atualizações "KBs" da Microsoft para ambientes Windows. Além disso, o sistema deve permitir a criação de uma lista de equipamentos autorizados, utilizando filtros como MAC-Address ou Hostname, e incluir restrições adicionais baseadas em registros do sistema (registry) do Windows. As condições descritas poderão ser aplicadas individualmente ou combinadas, conforme a necessidade da contratante;

r) Suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12[2];
s) Suportar a leitura e verificação de CRLs (certification revogation lists), e;
t) Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL/TLS.

1.2.12. Funcionalidades de Prevenção de Perda de Dados (Data Loss Prevention)

a) Evitar vazamento de informações em meio digital (Data Loss Prevention - DLP), atuando de maneira preventiva por meio do monitoramento de mensagens e arquivos transitados, e;
b) Caso seja identificado algum conteúdo que não deve ser transitado, a solução deve alertar o usuário que este conteúdo é sensível, ou mesmo bloquear o tráfego associado, baseado em filtros de conteúdo definidos pelo contratante.

1.2.13. Características da alta disponibilidade:

a) Deve operar em alta disponibilidade (HA) nativamente no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo, com sincronismo de estados integrado;
b) Suportar o balanceamento de carga interno na arquitetura ativo/ativo, disponibilizando a capacidade agregada dos dois equipamentos no cluster;
c) Suportar, no mínimo, 2 equipamentos por cluster. No caso de uso de três equipamentos será permitido que um permaneça em stand by;
d) Deve sincronizar entre os nós do Cluster todas as configurações recursos necessários para que a solução mantenha o funcionamento pleno em caso de falha de um dos equipamentos, como conexões e sessões TCP/IP, tabelas NAT, listas e assinaturas utilizadas para controle de acesso à Internet e proteção contra ameaças, tabelas FIB, associações de segurança das VPNs, entre outros.
e) Monitorar a falha dos links de comunicação e entre os nós do cluster;
f) Identificar e transferir automaticamente a operação do sistema (procedimento de failover) sempre que ocorrer: Falha de um cluster (quando existirem mais de um cluster instalado no contratante), transferindo a carga para o outro em data center distinto. Falha de um dos membros do cluster. Falha de qualquer componente ou processo crítico de um dos membros do cluster. Falha de um dos links de comunicação monitorados, e;
g) Deve ser capaz de realizar os procedimentos de failover sem perda das conexões ativas e interrupções no tráfego.

1.2.14. Funcionalidades para tratamento de ameaças desconhecidas (Zero-Day)

a) Deve contemplar ferramenta compatível com conceito de Sandboxing para prevenção de ataques zero-day;
b) Prevenção de ataques por meio do bloqueio efetivo de malwares desconhecidos (Dia Zero), oriundos da comunicação Web (HTTP e HTTPS), FTP, SMTP e IMAP/POP3 durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente;

[2] O PKCS #12 faz parte da família de padrões chamados Public-Key Cryptography Standards (PKCS) publicados pela RSA Laboratories. Esse padrão de criptografia define um formato de arquivo para armazenar muitos objetos de criptografia como um único arquivo. E tal arquivo é usado para agrupar uma chave privada com seu certificado X.509 ou todos os membros de uma cadeia de confiança.

c) O envio de conteúdo para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;
d) A funcionalidade de Sandbox deverá ser implementada em nuvem, appliance físico ou em ambiente virtual.
e) Caso a solução de Sandbox seja disponibilizada em ambiente virtual, é de responsabilidade da contratada providenciar servidores e softwares necessários para o funcionamento da ferramenta.
f) Deve ser capaz de enviar para análise, no mínimo, arquivos tipo Executável, PDF, DLLs, Arquivos de Código e MSI;
g) Suportar a análise de arquivos maliciosos em ambiente emulado e controlado com, no mínimo, os sistemas operacionais Windows 10 ou superior, Mac OS X ou superior;
h) Ser capaz de inspecionar e prevenir malwares desconhecidos em tráfego criptografado SSL/TLS;
i) Manter a performance sem degradação, independentemente das funcionalidades ativadas. (Ex.: AntiMalware, IPS, URL Filtering, e demais);
j) Geração de relatórios decorrentes das análises de links em Sandbox em caso de identificação de malwares e sites hospedeiros de exploits;
k) Deve ser capaz de classificar sites falsos, e atualizar a base do filtro URL da solução, e;
l) Deve prover análise em tempo real de páginas maliciosas e dessa forma, permitir o bloqueio de páginas maliciosas antes mesmo da atualização das bases de dados de URLs do fabricante da solução.

1.2.15. Administração e Gerência centralizada da solução de Next Generation Firewall.

1.2.15.1. A solução centralizada deverá gerenciar, de forma integrada, todos os equipamentos dos Grupos I e II que terão a renovação de garantia estendida ou que o órgão vier a adquirir, em qualquer combinação e quantidade dentro dos limites registrados.

1.2.15.2. A solução de gerenciamento centralizado deverá ser composta por, pelo menos, 1 (um) “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.

1.2.15.3. Será instalada em ambiente de virtualização e hardware de propriedade do contratante.

1.2.15.4. A Licença de Software para administração / gerência deve estar disponível, para uso, integrada com a base de identificação de usuários do contratante, em até 60 dias da comunicação da assinatura do contrato.

1.2.15.5. A solução de gerência terá atualização e suporte pelo período de 60 meses a contar do seu recebimento definitivo. Deverá permitir sua utilização por tempo indeterminado, em sua última versão disponível na data do encerramento do período de 60 meses.

1.2.15.6. A solução de gerência deverá ser separada dos gateways de segurança, que irão gerenciar políticas de segurança de todos os Firewalls e funcionalidades solicitadas neste documento.

1.2.15.7. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução.

1.2.15.8. Possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos gerenciados via plataforma de segurança.

1.2.15.9. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento.

1.2.15.10. Suportar acesso via SSH para gerência, via cliente do próprio fabricante ou WEB (HTTPS).

1.2.15.11. O gerenciamento deve permitir/possuir monitoramento de logs, ferramentas de investigação de logs e acesso concorrente de administradores via contas diferentes.

1.2.15.12. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comando

1.2.15.13. A solução deve suportar a criação de regras com agendamento personalizado, permitindo configurar datas e horários de início e término para o uso de cada regra.

1.2.15.14. Suportar backup das configurações e reversão (rollback) de configuração, pelo menos, para a última configuração salva.

1.2.15.15. Suportar validação de regras antes da aplicação.

1.2.15.16. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras já existentes (shadowing).

1.2.15.17. Permitir a visualização dos logs em tempo real de uma regra específica, diretamente na mesma tela de configuração da regra selecionada, garantindo uma experiência integrada e facilitando o monitoramento e a análise imediata do tráfego associado.

1.2.15.18. Possibilitar a integração com, no mínimo, as soluções de SIEM IBM Qradar e Trend One, ferramentas que compõe a solução de monitoramento, detecção, notificação, investigação e resposta a ataques cibernéticos que compõem a Ata de Registro de Preços n.20/2024, vigente, resultante do Pregão Eletrônico n.30/2024 - PROAD n. 22.093/2024 do TRT 2, contratada por vários órgãos participantes do presente processo.

1.2.15.19. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

1.2.15.20. Permitir a criação de certificados digitais para autenticação de usuários.

1.2.15.21. Geração de relatórios de todas as funcionalidades de segurança que estão ativadas nos GW’s de segurança. Deve permitir apresentar eventos em um único portal (dashboard). Também devem existir relatórios e telas de apresentação onde sejam apresentados os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing).

1.2.15.22. Permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

1.2.15.23. Permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0.

1.2.15.24. Permitir que os administradores consigam revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

1.2.15.25. Permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

1.2.15.26. Registrar logs, correlação de eventos e relatórios de auditoria dos administradores da solução.

1.2.15.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados.

1.2.15.28. Permitir a criação de relatórios personalizados.

1.2.15.29. Permitir criar relatórios com o resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de usuários específicos e grupos de usuários do AD/LDAP. Os relatórios de usuários e grupos devem incluir as aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware) de rede vinculadas a este tráfego.

Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução.

1.2.15.30. Possibilitar exportação dos logs em formatos CSV ou TXT.

1.2.15.31. Aplicar separadamente proteções relacionadas a ameaças e regras de acesso.

1.2.15.32. Para evitar erros na alteração de políticas, a solução deve combinar configuração de políticas e análise de logs em um único painel.

1.2.15.33. O visualizador de log deve ter um recurso de pesquisa.

1.2.15.34. Possibilitar a geração de relatórios de eventos no formato PDF ou HTML.

1.2.15.35. Possibilitar rotação do log.

1.2.15.36. O gerenciamento centralizado deverá ser entregue como appliance virtual em formato compatível/homologado com tecnologia VMWare ESXi.

1.2.15.37. A solução de gerenciamento deve possuir a capacidade de gerenciar outros Firewalls de segurança do mesmo fabricante mesmo estão em ambientes físicos (on premises), virtualizados e nuvens públicas (AWS e Azure) e nuvens privadas (VmWare NSX ou Cisco ACI).

1.2.15.38. Possuir capacidade de integração com soluções de terceiros via API e suportar configurações por meio de RestAPI.

1.2.15.39. Consolidar logs e relatórios de todos os dispositivos administrados pela gerência integrada.

1.2.15.40. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura.

1.2.15.41. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real.

1.2.15.42. Nas opções de Drill-Down deve ser possível identificar os acessos específicos de cada usuário.

1.2.15.43. Permitir que os relatórios possam ser salvos, enviados por e-mail e impressos.

1.2.15.44. Deve permitir a criação de filtros na visualização on-line dos relatórios com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

1.2.15.45. Permitir visualização via painel de gerência on-line da quantidade de tráfego utilizado de aplicações e navegação para permitir análise avançada de incidentes.

1.2.15.46. Gerar relatório dos eventos de ataque de forma completamente visual, contendo, no mínimo, gráficos de consumo de banda utilizado pelos ataques e quantidade de eventos de segurança gerados e também eventos de segurança protegidos.

1.2.15.47. Permitir a integração com servidores de autenticação por meio dos serviços de diretório OpenLDAP com protocolo LDAP, Microsoft Active Directory e servidores RADIUS.

1.2.15.48. Criar certificados digitais para acesso dos usuários VPN.

1.2.15.49. Criar certificados digitais para VPNs Site-to-Site.

1.2.15.50. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplada a sua maior capacidade ou a capacidade de criação de certificados deve ser ilimitada.

1.2.15.51. Permitir criação de políticas de acesso de usuários autenticados por meio dos serviços de diretório OpenLDAP com protocolo LDAP e Microsoft Active Directory, de forma que os usuários sejam reconhecidos de forma transparente.

1.2.15.52. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças classificadas por origens e destinos do tráfego de dados.

1.2.15.53. Possibilitar a visualização dos logs de Firewall, navegação web, conteúdo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado, permitindo a procura correlacionada de logs em uma única tela, como por exemplo: pesquisar logs de Antivírus e navegação web simultaneamente na mesma consulta (query de pesquisa).

1.2.15.54. O relatório das emulações (sandboxing) deve conter deve conter um dos seguintes conjuntos de informações:

a) Print screen dos arquivos emulados, todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações individualizado para cada SO emulado, ou;
b) Tipo do arquivo, tamanho do arquivo, nome do arquivo, hash do arquivo, usuário que o recebeu, o veredito (um arquivo malicioso, um arquivo não malicioso e um arquivo não malicioso, mas com características indesejáveis que deixam o sistema operacional lento ou que alteram parâmetros do sistema).

1.2.15.55. Possibilitar a procura por IPs e redes, de forma que os resultados mostrem estes IPs e redes nos campos de origem e destino dos logs na mesma tela de pesquisa;

1.2.15.56. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

1.2.15.57. Capacidade de personalização de gráficos com os dados dos logs, como barra, linha e tabela;

1.2.15.58. Permitir a criação de painéis (dashboards) customizados para visualização do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

1.2.15.59. Possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema e dos componentes gerenciados por ele, contendo, no mínimo, licenças ativas, utilização de memória, utilização de discos e uso de CPUs;

1.2.15.60. Ser capaz de correlacionar eventos de todas as suas fontes de log em tempo real;

1.2.15.61. Fornecer conteúdo de correlação de eventos pré-definido organizado por categoria;

1.2.15.62. Monitorar alterações, análise e otimização de regras de políticas de segurança;

1.2.15.63. Possibilitar a verificação de regras de acesso por meio de uma consulta de origem, destino e serviço, a solução também deve apresentar se o tráfego está permitido, bloqueado ou parcialmente permitido/bloqueado, demonstrando os dispositivos no caminho, roteamento e interfaces;

1.2.15.64. Deve apresentar relatórios de otimização de regras e objetos, no mínimo, contendo as seguintes informações:

a) Regras não usadas;
b) Regras cobertas
c) Consolidar regras
d) Regras desabilitadas
e) Regras temporárias (definição de data e hora de funcionamento)
f) Regras mais usadas;
g) Última vez que uma regra foi usada;
h) Objetos duplicados;
i) Objetos vazios, e;
j) Serviços duplicados.

1.2.15.65. Permitir a monitoração de itens de configuração do sistema operacional dos dispositivos gerenciados;

1.2.15.66. Enviar alertas configuráveis sobre regras a expirar;

1.2.15.67. Emitir alertas em caso de alterações de configuração que não estão em conformidade com os padrões e políticas corporativas vigentes;

1.2.15.68. Realizar a comparação das configurações de um mesmo ou entre diferentes dispositivos;

1.2.15.69. Permitir o agendamento para a geração de relatórios dos dispositivos gerenciados;

1.2.15.70. Ser capaz de fornecer lista de usuários de VPN dos dispositivos gerenciados, no mínimo, baseados nos seguintes critérios:

a) Data de criação;
b) Grupos de usuários;
c) Métodos de autenticação dos usuários, e
d) Data de expiração dos usuários.

1.2.15.71. A comunicação entre a solução e os dispositivos de segurança gerenciados deve ser autenticada e criptografada;

1.2.15.72. Capacidade de comparar a base de regras do firewall com baselines padrão de mercado e fornecer um relatório de conformidade com o padrão utilizado na comparação;

1.2.15.73. Capacidade de migrar as regras e políticas dos dispositivos instalados nos contratantes para dispositivos substitutos, mesmo que de modelo e fabricante diferentes, utilizando a gerência ou ferramenta de terceiros.

1.2.15.74. Qualquer alteração na configuração dos dispositivos deve ser identificada automaticamente contendo as seguintes informações:

a) Qual foi a alteração;
b) Quem efetuou a alteração;
c) A data e hora da alteração;
d) Cada alteração nos dispositivos, deve ser identificado, no mínimo:
e) Alterações nas Regras (Criação, Remoção, Modificação);
f) Alteração nos Objetos de Redes e Serviços;
g) Alterações de Rotas ou Interfaces, e;
h) Visibilidade de toda alteração de configuração nos dispositivos.

1.2.15.75. O sistema deve realizar validação contínua das políticas e controles de segurança por meio de simulações em ambiente real; Deve possuir suporte de integração com plataformas de SIEM, permitindo análise e correlação de eventos em tempo real;

1.2.15.76. Possuir uma biblioteca de ameaças atualizada diariamente, contendo, no mínimo, 15.000 técnicas de táticas e procedimentos (TTPs) e 3.000 tipos de ameaças, incluindo exploits de vulnerabilidades e ataques APTs;

1.2.15.77. Possibilitar geração de relatórios personalizados que evidenciem mudanças na postura de segurança ao longo do tempo, incluindo recomendações específicas para mitigações baseadas no fornecedor e no cenário da ameaça;

1.2.15.78. Compatibilidade com ferramentas de segurança de rede, incluindo integração com plataformas de mercado para gestão de segurança;

1.2.15.79. Licenciamento das funcionalidades especificadas no Edital para os equipamentos (appliances)

1.2.16. Todas as funcionalidades descritas para a solução de Next Generation Firewall devem estar devidamente licenciadas e disponíveis para uso durante todo o período do contrato. Sendo elas, Application Control, identificação de usuários, firewall, geolocalização, navegação internet e inspeção de tráfego SSL/TLS, IPS, VPN, ameaças zero-day, sandboxing, logging, gerência centralizada, SD-WAN (caso contratada via Itens 10 e 11 do Edital) e demais funcionalidades necessárias para completa utilização dos equipamentos.

1.2.17. Instalação do Cluster Grupo I

Os novos equipamentos adquiridos ou os equipamentos a serem substituídos por estarem em end-of-support deverão ser instalados seguindo o planejamento definido nesta subseção.

1.2.17.1. Requisitos Gerais da Instalação

1.2.17.1.1. Caberá à contratada todo o processo de planejamento, a instalação, a configuração, os testes, a migração e a compatibilidade dos equipamentos, que deverão ser integrados à infraestrutura de Tecnologia de Informação existente no local de instalação dos equipamentos, como switches, roteadores, equipamentos servidores, entre outros.

1.2.17.1.2. O processo de instalação, configuração, testes e migração deve acontecer em até 90 dias corridos após a comunicação da assinatura do contrato no caso de aquisição de novos equipamentos. Nos casos onde for decretado end-of-support para equipamentos dentro do prazo de vigência do contrato de garantia, o processo de instalação, configuração, testes e migração do equipamento a ser substituído deve ter como marco inicial a notificação da empresa sobre a necessidade de troca dos equipamentos.

1.2.17.1.3. A atividade de janela para efetiva entrada em produção do novo equipamento da solução de Firewall deverá ser agendada pelo contratante.

1.2.17.1.4. A contratada deverá realizar uma avaliação preliminar do ambiente de TI da contratante, incluindo uma análise da infraestrutura atual, para identificar quaisquer pré-requisitos ou necessidades de adaptação antes da implementação.

1.2.17.1.5. A Instalação terá quatro marcos: Reunião de Alinhamento Inicial; Entrega do Plano de Trabalho; Execução da instalação, migração e testes; Efetiva entrada em produção do novo equipamento.

1.2.17.1.6. A contratada é responsável pela instalação completa e configuração dos equipamentos e software, garantindo que estes estejam operacionais e otimizados para o ambiente da contratante.

1.2.17.1.7. A contratada deverá manter um canal de comunicação com a contratante durante a instalação/migração.

1.2.17.2. Requisitos de Instalação/migração

1.2.17.2.1. A instalação/migração não deve interromper as operações diárias da contratante sem agendamentos prévios e deve ser feita de forma a minimizar qualquer possível tempo de inatividade.

1.2.17.2.2. Eventuais necessidades de interrupção devem ser autorizadas e agendadas com a Administração do Órgão, com possibilidade de serem realizadas em finais de semana.

1.2.17.2.3. A instalação/migração envolverá as seguintes atividades:

a) Reunião de Alinhamento Inicial:
    i) A reunião de alinhamento inicial deverá ocorrer em até 15 dias da comunicação da assinatura do contrato.
    ii) Neste momento, a contratante deverá informar se a contratada deverá realizar

a migração das configurações de solução de Firewall já instaladas, ou se prefere instalar uma configuração totalmente nova.

b) Entrega do Plano de Trabalho (Cronograma e Escopo):
   i) O Plano de Trabalho deverá contemplar ao menos: Declaração de Escopo, Matriz RACI, Cronograma (datas da Instalação Física e Lógica e Efetiva entrada em produção do novo equipamento), Recursos Humanos, procedimentos e testes a serem realizados no final da instalação
   ii) O documento em PDF deverá ser enviado para o Gestor e o Fiscal Técnico em até 15 dias da reunião de alinhamento inicial.
   iii) A contratante terá 10 dias para analisar o documento, realizando, por e-mail, as solicitações que entender cabíveis.
   iv) Sendo necessárias alterações a contratada terá 5 dias para apresentar, também por e-mail, a versão final.

c) Execução da instalação, migração e testes:
   i) Esta etapa terá início após a entrega dos equipamentos e deverá ser concluída em até 90 dias da comunicação da assinatura do contrato.
   ii) A contratada deverá disponibilizar o acompanhamento "on site" durante a instalação de, pelo menos, um especialista, certificado pelo fabricante do equipamento, para ser responsável pela execução da instalação, migração e testes, pelo tempo necessário, com, no mínimo, 40 horas de trabalho (sem contar a uma hora diária de almoço), sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h;
   iii) Caso a instalação não seja concluída no período citado no item anterior, deverá haver um especialista técnico, em esquema de atendimento remoto, sendo o limite de 9 horas diárias (incluindo uma hora para almoço), no horário das 8h às 17h, que poderá ser acionado via telefone celular, até o recebimento definitivo do serviço de instalação.
   iv) A instalação física compreende a fixação, conexão de cabos de energia e lógicos de forma a possibilitar o funcionamento da solução de Cluster nas dependências do contratante
   v) Todas as conexões elétricas e lógicas utilizadas deverão ter seus cabos (rede, óticos e/ou elétricos) identificados (etiquetagem), sendo a contratada responsável pelo fornecimento e impressão das etiquetas e materiais necessários para a organização, como presilhas, velcros, entre outros.
   vi) A instalação lógica se inicia com a preparação dos equipamentos com sua última versão estável com seus patches (releases) mais recentes instalados. Não serão aceitas funcionalidades que estejam executando em builds não-estáveis (alpha, beta etc.) ou modificações personalizadas diretamente em código.
   vii) Quando solicitado pela contratante na reunião de alinhamento, a instalação compreenderá a migração das configurações e regras existentes no ambiente atual do contratante, suportado por um cluster de firewalls que pode ser de fabricante distinto da solução ofertada, assim como as demais configurações de segurança e disponibilidade.
   viii) Transferência das configurações da solução atual para o novo equipamento, além de criação de novas regras e políticas que se mostrarem necessárias. Preferencialmente, o processo deverá ocorrer em ambiente apartado do ambiente produtivo, em uma rede virtual (VLAN) distinta do ambiente produtivo para que não haja influência na operação;
   ix) Validação dos dados criados nos novos equipamentos comparando-os com os dados dos equipamentos legados, garantindo a integridade das configurações;
   x) Configuração lógica do equipamento para comunicação deste com a rede de

dados da contratante.

xi) Realização dos testes especificados no item 1.2.17.2.4.

xii) Ao final da etapa de Execução da instalação, migração e testes, deverá ser enviado, para o e-mail do Gestor e do fiscal técnico, o Arquivo de configurações dos novos equipamentos.

d) Efetiva Entrada em Produção do Novo Equipamento:
   i) Esta data deverá ser alinhada e autorizada pelo Gestor do contrato.

1.2.17.2.4. Testes

No intuito de validar o funcionamento das configurações realizadas, incluindo migração, devem ser realizados, no mínimo, os seguintes testes:

a) Deverá ser feito, no mínimo, dois tipos de acesso a partir da rede interna para a rede Servidores e para a rede DMZ.
   i) Acesso 1: utilizando protocolo https e sendo liberado o acesso, e;
   ii) Acesso 2: utilizando protocolo ssh e sendo bloqueado para a DMZ é liberado para a rede servidores;

b) Deverá ser feito um tipo de acesso externo com origem em um cliente VPN com destino a rede servidores.

c) Deverá ser exibido na console de gerência os registros que demonstrem:
   i) O horário da aplicação das últimas políticas;
   ii) A mudança realizada para bloqueio do Facebook;
   iii) O horário da mudança, e;
   iv) O administrador que realizou a mudança;

d) Deve ser desligada a PDU do nó ativo;
   i) Verificar se o nó passivo assumiu as operações com RTO[3]=0 (zero);
   ii) Ligar o appliance do nó ativo, e;
   iii) O nó ativo deverá assumir o controle das operações.

1.3. Características comuns para - Serviço de garantia e atualização de assinaturas de proteção e suporte técnico em regime 24x7 por 60 meses para solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall, com alta disponibilidade, incluindo software de administração e gerência integrada - Grupo I Item I (Equipamentos Tipo I)

1.3.1. Os serviços de assistência técnica “on-site”, realizados pela contratada ou autorizados pela mesma mediante declaração expressa, deverão ser prestados em Belo Horizonte – MG.

1.3.2. Todos os custos e encargos relacionados à execução dos serviços de garantia e assistência técnica necessários durante o prazo de garantia dos serviços e dos bens serão de responsabilidade integral da contratada.

1.3.3. A contratada deverá prestar serviço de manutenção e suporte técnico ao longo da vigência do contrato destinado a:

[3] RTO (Recovery Time Objective) é a sigla em inglês para Objetivo de Tempo de Recuperação. É uma métrica que define o tempo máximo que um sistema pode ficar inativo após uma interrupção

a) Restabelecimento de serviços interrompidos ou degradados;
b) Solução de problemas de configuração e falhas técnicas nos serviços;
c) Esclarecimentos de dúvidas sobre configurações e utilização dos serviços, e;
d) Implementação de novas funcionalidades.

1.3.4. A garantia e serviço de assistência técnica do produto ofertados deverão ser do Fabricante.

1.3.5. A assistência técnica da garantia consiste na reparação das eventuais falhas dos equipamentos, mediante a substituição de peças, componentes e acessórios que se apresentem defeituosos de acordo com os manuais e normas técnicas específicas para os equipamentos. No caso do modelo do equipamento haver sido descontinuado, um similar será aceito, desde que possua as características técnicas iguais ou superiores às exigidas no Edital.

1.3.6. O serviço de garantia deverá abranger os defeitos de hardware e de software, através de manutenção preventiva ou corretiva, incluindo a substituição de peças, partes, componentes e acessórios, sem representar quaisquer ônus para o Tribunal.

1.3.7. Os equipamentos devem contar com garantia de funcionamento, atualização de assinaturas de proteção e assistência técnica do fabricante, além do suporte técnico local e remoto pela Contratada, 24x7 (vinte e quatro horas por dia, sete dias na semana), pelo prazo de 60 (sessenta) meses.

1.3.8. Todas as partes e peças deverão ser substituídas pelos serviços de garantia, através de funcionários habilitados e credenciados para tal. Não serão aceitos o envio de peças/equipamentos pelos Correios, para que haja substituição por parte do Contratante. O Contratante não se responsabiliza por quaisquer danos aos equipamentos, que possam vir a ocorrer caso seja utilizada a prática de postagem pelos Correios.

1.3.9. Toda e qualquer substituição de peças e componentes deverá ser acompanhada por funcionário designado pelo Contratante, que autorizará a substituição das peças e componentes, os quais deverão ser novos e originais.

1.3.10. Em caso de necessidade de nova instalação e/ou configuração os serviços deverão ser realizados pela Contratada ou pelo Fabricante, por técnico certificado com capacidade técnica para a realização do serviço comprovada através da apresentação de documento de certificação emitido pela própria fabricante do equipamento ou por empresa de treinamento reconhecida pelo fabricante. Se necessário, a documentação original ou “as built” deverão ser atualizados pela contratada.

1.3.11. Os serviços de suporte que porventura implicarem na necessidade de desligamento de outros equipamentos, como servidores, storage, links, etc., deverão ser executados, preferencialmente, em horários fora do expediente, podendo inclusive ocorrer em finais de semana ou feriados, a critério do contratante.

1.3.12. A contratada deverá ter acesso completo aos Fóruns de Produtos do fabricante durante a vigência do contrato;

1.3.13. A contratada deverá ter acesso à base de conhecimento de suporte online do fabricante durante a vigência do contrato;

1.3.14. A contratada deverá ter cadastrado em portal do fabricante para download de firmwares, patches e softwares que fazem parte ou complementam a solução;

1.3.15. Serão aceitos modelo de suporte híbrido, em que os primeiros níveis são atendidos pela contratada e os últimos níveis pelo fabricante.

1.3.16. Níveis de Gravidade dos chamados para definição de tempos de atendimento.

1.3.16.1. Gravidade 1

a) Um erro com impacto direto na segurança do produto;
b) Um erro isolado no software ou dispositivo em um ambiente de produção que torna o produto inoperante; por exemplo, impacto crítico no sistema, queda do sistema;
c) Um defeito relatado no produto em um ambiente de produção, que não pode ser razoavelmente contornado, em que haja uma condição de emergência que restrinja significativamente o uso, como por exemplo, PJe fora do ar por problemas de configuração do sistema Firewall;
d) Produto para de executar as funções de negócios necessárias, como interrupção no acesso à Internet via rede Interna; ou
e) Incapacidade de usar o equipamento ou qualquer outro impacto crítico na operação do Firewall que exija uma solução imediata.

1.3.16.2. Gravidade 2

a) Um erro isolado no software ou no equipamento que degrade substancialmente o desempenho dos sistemas de TIC que dependem dele, por exemplo, Sistema PJe acessível mas com performance muito degradada, lento e/ou com funcionalidades limitadas devido problemas de Firewall;
b) Um defeito que restringe o uso de um ou mais recursos mas não chega a afetar completamente o uso do Firewall, ou;
c) A utilização de uma função importante não está disponível e as operações são gravemente impactadas; por exemplo, lentidão nos sistemas da rede interna acessados via Internet.

1.3.16.3. Gravidade 3

a) Um erro isolado no Firewall que causa apenas um impacto moderado no uso do produto; por exemplo, Demora no login de sistemas via Internet, demora em algumas operações específicas do PJe, intermitência entre lentidão e desempenho satisfatório;
b) Um defeito que restringe o uso de um ou mais recursos do produto licenciado mas pode ser facilmente contornado, como parada do funcionamento da navegação Internet via rede Interna com autenticação de usuário e senha, mas que pode funcionar normalmente se liberada a autenticação até o problema ser resolvido, ou;
c) Um erro que pode causar algumas restrições funcionais, mas não tem um impacto crítico ou severo nas operações, como parada no acesso a sites de compra on-line.

1.3.16.4. Tempos de atendimento

Os tempos de atendimento estão descritos na tabela TR3, conforme segue.

Tabela A3 - Tempos de atendimento o Serviço de atualização de garantia

Serviço	**Tempo e condições**
Regime do atendimento	24x7
Tempo de resposta comprometido para problemas de Gravidade 1 (1)	30 minutos
Tempo de resposta comprometido para problemas de Gravidade 2 e 3 (1)	Gravidade 2 - 2 horas Gravidade 3 - 4 horas
Remessa de equipamentos em caso de necessidade de troca (RMA)	Próximo voo de saída/entrega expressa (quando aplicável) ou remessa no mesmo dia útil (2)

(1) Entende-se cumpridos os 30 minutos de tempo de atendimento caso haja comunicação em tempo real (chat, telefone). (2) Equipamentos são enviados durante o horário comercial normal e podem chegar fora do horário comercial.

1.3.17. A Contratada deverá providenciar o deslocamento de peças ou equipamentos para substituição bem como seu retorno sem qualquer ônus à contratante.

1.3.18. Todas as peças ou componentes utilizados/substituídos nos reparos deverão ser originais do fabricante, sem uso anterior e possuir, no mínimo, o mesmo desempenho e as mesmas garantias daqueles originalmente fornecidos.

1.3.19. Em caso de novos equipamentos, os mesmos devem ser compatíveis com os demais ativos de data center de cada Órgão participante. Ficará a cargo da contratada a verificação de compatibilidade antes da efetivação da reposição. Caso o sistema ofertado não tenha sua compatibilidade verificada, o correto funcionamento de todas as funcionalidades do sistema ofertado será de inteira responsabilidade da contratada, que deverá empreender todos os esforços necessários para entregar o sistema em pleno funcionamento, sob pena de arcar com as multas contratuais relativas a quebra de contrato.

1.3.20. Caso o equipamento não possa ser reparado dentro do prazo previsto, deverá ser providenciada pela contratada a instalação, em caráter provisório, de equipamento equivalente ou de configuração superior até que seja sanado o defeito do equipamento em reparo.

1.3.21. Caso os serviços de assistência técnica da garantia não possam ser executados nas dependências do contratante, o equipamento avariado poderá ser removido para o centro de atendimento da contratada. A contratada deverá fazer a justificativa por escrito relacionando os problemas apresentados que deverá ser apresentada ao setor competente do contratante que fará o aceite e providenciará a autorização de saída do equipamento, desde que o mesmo seja substituído por outro equivalente ou de superior configuração, durante o período de reparo. O equipamento retirado para reparo deverá ser devolvido no prazo de 5 (cinco) dias úteis contados a partir da sua retirada.

1.3.22. A devolução de qualquer equipamento retirado para reparo deverá ser comunicada por escrito ao contratante.

1.3.23. A contratada deverá substituir o equipamento já instalado, por um novo e de primeiro uso, no prazo máximo de 2 (dois) dias corridos, na hipótese do mesmo equipamento apresentar defeito por 2 (duas) ou mais vezes dentro de um período de 20 (vinte) dias corridos.

1.3.24. Caso os equipamentos cobertos pelo serviço de garantia, atualização de assinaturas de proteção e suporte técnico vierem a ser declarados pelo fabricante em listas de end-of-life, end-of-support e/ou end-of-sale com essas datas terminando antes do período de vigência do contrato, os mesmos deverão ser substituídos pelos novos equipamentos indicados pelo fabricante em seu site, esses equipamentos devem ter capacidade idêntica ou superior ao equipamento antigo e possibilitar o uso de todas as funcionalidades do equipamento anterior.

1.3.25. Os serviços dependentes de atualização pela Internet e cujas licenças serão vinculadas à vigência do contrato, são: controle de acesso à Internet (controle de aplicações e filtragem de URLs), prevenção de ameaças (IPS, Antivírus, Anti-Bot, Anti-Malware, Anti-Spyware), prevenção de perda de dados (data loss prevention) e postura dos endpoints, e demais funcionalidades necessárias para completa utilização dos equipamentos.

1.3.26. O licenciamento deverá permitir a utilização da solução, por tempo indeterminado, em sua última versão disponível na data do encerramento dos serviços de garantia, suporte técnico e atualização de versões.

1.3.27. Vigência e início do contrato
Para equipamentos já instalados a garantia deve iniciar em até 10 dias após a comunicação da assinatura do contrato. Para novos equipamentos os serviços de garantia e atualização terão vigência de 60 meses com início a partir da emissão do termo de recebimento definitivo da ativação de licenças vinculadas aos equipamentos Firewall Tipo I (Grupo I Item I).

ANEXO II - Endereço de Entrega/Prestação dos Serviços

Nome do órgão:	Tribunal Regional do Trabalho da 3ª Região
UG/UASG:	080008
CNPJ:	01.298.583/0001-41
Unidade responsável pela fiscalização:	Secretaria de Infraestrutura Tecnológica
Servidor responsável:	Marden Pacheco Oliveira Diniz
Telefone:	(31) 3238-7908
E-mail:	marden@trt3.jus.br
Endereço da prestação dos serviços/ entrega dos equipamentos:	Rua Mato Grosso, 400 - Barro Preto - BH - MG

ANEXO A - "Termo de Confidencialidade e de Responsabilidade"

Eu, (nome do profissional contratado), Inscrito no Cadastro de Pessoa Física(CPF) número (número do CPF do profissional), denominado PROFISSIONAL CONTRATADO da empresa (nome da empresa contratada),CNPJ (CNPJ da empresa contratada), denominada EMPREGADORA, declaro estar ciente das disposições abaixo, com as quais concordo plenamente.

O PROFISSIONAL CONTRATADO compromete-se a manter no mais absoluto sigilo e confidencialidade todas as informações do Tribunal Regional do Trabalho da 12ª Região, que, por qualquer meio, direta ou indiretamente, tomar conhecimento em razão dos serviços ora contratados.

O PROFISSIONAL CONTRATADO poderá ter acesso e conhecimento de informações e dados disponíveis do Tribunal Regional do Trabalho da 12ª Região, incluindo informações relativas aos servidores e magistrados, processos administrativos e judiciais, atividades de pesquisa, engenharia e desenvolvimento, tecnologia, pesquisa e métodos de processamento de dados, listas de usuários dos sistemas, dados sobre andamento processual, fornecedores, produtos, processos, listas de autores e réus em ações trabalhistas, informações financeiras, organizacionais, entre outros, devendo manter todas as informações em sigilo absoluto.

O PROFISSIONAL CONTRATADO tem ciência de que o tratamento dos dados a que poderá ter acesso, na forma como é descrito no art. 5º da Lei nº13.709/2018 – LGPD, será realizado exclusivamente nos limites e finalidades previstos no presente contrato. Declaro estar ciente de que, pela inobservância do acima exposto, poderei responder civil, penal e administrativamente, nos termos da lei.