ATO CONVOCATÓRIO Nº 08/2025
REQUISIÇÃO DE COMPRAS Nº 10005034

CONTRATANTE:
Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos (Cebraspe)

OBJETO:
O Registro de Preços para futura aquisição de Solução de Segurança de Rede com características de Next Generation Firewall (NGFW) composta por hardware e software, com serviço especializado de instalação, integração, armazenamento de logs, com licenciamento e suporte do fabricante por 36 (trinta e seis) meses para uso nas dependências do Cebraspe.

PERÍODO DE ACOLHIMENTO DE PROPOSTAS
As propostas poderão ser enviadas no período de 22/12/2025 a 29/12/2025, até às 23h55min.

Envio das propostas:
E-mail: cplcebraspe@cebraspe.org.br

Contato para esclarecimentos: Telefone: (61) 2109-5741

CRITÉRIO DE JULGAMENTO:
O critério de julgamento adotado será o menor preço global, observadas as exigências contidas neste ato convocatório e seus Anexos quanto às especificações do objeto.

ANEXOS

I – Modelo de Propostas
II – Modelo de Declaração de Menor e Parentesco
III – Minuta de Contrato
IV – Termo de referência e anexos

ATO CONVOCATÓRIO Nº 08/2025
REQUISIÇÃO Nº 10005034

O Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos (Cebraspe), com sede no SETOR DE ABASTECIMENTO E ARMAZENAGEM NORTE(SAAN), QUADRA 01 LOTES 1095, 1105, 1115, 1125, 1135 E 1145, ZONA INDUSTRIAL – Brasília/DF associação civil de direito privado, sem fins lucrativos e substituto tributário, portanto está obrigado à retenção de tributos federais (INSS, IRRF, PIS, COFINS e CSLL) e no âmbito distrital do Imposto Sobre Serviços de Qualquer Natureza (ISSQN), incidentes sobre os serviços contratados, com base nas legislações específicas vigentes, quando couber, incumbida da pesquisa, do ensino e do desenvolvimento institucional na área da educação, inscrita no CNPJ nº 18.284.407/0001-53, torna público que fará realizar certame seletivo, na modalidade de **REGISTRO DE PREÇOS,** do Tipo **MENOR PREÇO GLOBAL,** conforme descrito neste Ato convocatório e seus Anexos e de conformidade com as disposições contidas no Código Civil Brasileiro, no Regimento Interno e no Regulamento de Compras e Contratações do Cebraspe, aprovados pelas Resoluções nº 01, de 10 de janeiro de 2014 e nº 8, de 22 de agosto de 2018, respectivamente, do Conselho de Administração do Cebraspe.

1. DAS DISPOSIÇÕES PRELIMINARES

1.1. O processo de seleção de fornecedores será conduzido de forma pública, objetiva e impessoal, com observância dos princípios de publicidade, impessoalidade, moralidade, economicidade, eficiência, dentre outros, nos termos do Regulamento de Compras e Contratações do Cebraspe.

1.2. Este processo de seleção de fornecedores respeitará o disposto no Regulamento Próprio de Compras e Contratações do CEBRASPE, disponível no endereço eletrônico: https://www.cebraspe.org.br/transparencia/

2. DO OBJETO

2.1. O presente processo tem por objeto o Registro de Preços para futura aquisição de Solução de Segurança de Rede com características de Next Generation Firewall (NGFW) composta por hardware e software, com serviço especializado de instalação, integração, armazenamento de logs, com licenciamento e suporte do fabricante por 36 (trinta e seis) meses para uso nas dependências do Cebraspe, conforme especificações e quantidades constantes neste ato convocatório e seus anexos.

3. DAS CARACTERÍSTICAS DOS SERVIÇOS

3.1. A descrição técnica dos serviços está descrita no anexo I do termo de referência.

4. DO RECEBIMENTO DOS SERVIÇOS

4.1. O recebimento dos serviços compreenderá duas etapas distintas, a seguir discriminadas:

4.1.1. Provisoriamente, no prazo de até 1 (um) dia útil a partir da disponibilização do serviço, mediante termos próprios, para efeito de posterior verificação da conformidade dos serviços com a especificação prevista neste contrato;

4.1.2. Definitivamente, no prazo de até 5 (cinco) dias úteis a partir da disponibilização provisória dos canais, mediante atesto de nota fiscal, após a verificação da qualidade e quantidade dos serviços e consequente aceitação;

4.2. Em caso de não conformidade, lavrar-se-á Termo de Recusa e Devolução, no qual se consignarão as desconformidades com as exigências. Nessa hipótese, o serviço objeto deste termo será rejeitado, devendo ser substituído ou refeito no prazo de 10 (dez) dias, quando se realizarão novamente as verificações em conformidade com os itens 4.1.1 e 4.1.2;

4.3. À CONTRATADA caberá sanar as irregularidades apontadas no recebimento definitivo, submetendo a etapa impugnada a nova verificação, ficando sobrestado o pagamento até a execução do saneamento necessário, sem prejuízo da aplicação das sanções cabíveis, sendo que os custos da substituição e/ou reparo dos serviços rejeitados correrão exclusivamente a expensas da CONTRATADA;

4.4. O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho dos serviços fornecidos, cabendo-lhe sanar quaisquer irregularidades detectadas quando do recebimento.

5. DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

5.1. Encerrado o prazo para recebimento, serão analisadas as propostas, observando-se a compatibilidade do preço ofertado com o valor estimado para a contratação, bem como o atendimento às condições de habilitação previstas no ato convocatório e seus Anexos

5.2. As propostas serão classificadas em ordem crescente, de acordo com o preço global, considerando-se exclusivamente as propostas que atenderem de forma integral à descrição do objeto e às exigências estabelecidas neste ato convocatório e em seus Anexos.

5.3. O Certame Seletivo será disputado por lote.

6. DO PRAZO DE ACOLHIMENTO DE PROPOSTAS

6.1. O período de acolhimento das propostas será de 8 (oito) dias, contatos da publicação do ato convocatório no site oficial do CEBRASPE.

6.2. Envio de Propostas para o e-mail cplcebraspe@cebraspe.org.br
Contato: (61) 2109-5741

7. DAS CONDIÇÕES PARA PARTICIPAÇÃO

7.1. Poderão participar deste certame seletivo as empresas que explorem ramo de atividade compatível com o objeto deste certame seletivo, e que atendam às condições deste Ato convocatório e seus anexos, assim como apresentem os documentos nele exigidos.

7.2. O encaminhamento de proposta pressupõe o pleno conhecimento e atendimento às exigências de habilitação previstas no ato convocatório.

8. NÃO SERÁ ADMITIDA A PARTICIPAÇÃO DE EMPRESAS:

8.1. Que estejam sob falência, concurso de credores, concordata ou em processo de dissolução ou liquidação;

8.2. Que estejam suspensas do direito de contratar com a Administração Pública, ou que tenham sido declaradas inidôneas;

8.3. Que sejam reunidas em consórcio e sejam controladoras, coligadas ou subsidiárias entre si;

8.4. Estrangeiras que não estejam autorizadas a operar neste país;

8.5. Que estejam suspensas do direito de contratar com o Cebraspe;

8.6. Que esteja incluída no cadastro de empregadores que tenham submetido trabalhadores a condições análogas às de escravo, divulgado pela Controladoria-Geral da União (CGU), conhecido como “lista suja”;

8.7. Que não possua Classificação Nacional de Atividades Econômicas (CNAE) compatível com a natureza do fornecimento ou da prestação de serviço exigida, conforme a legislação vigente;

8.8. Que tenham participação, a qualquer título, de dirigentes ou empregados do Cebraspe, ou parentes destes, em linha reta ou colateral, até o terceiro grau;

8.9. Sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum.

9. DA PROPOSTA

9.1. Nas propostas a serem enviadas, deverão constar.

9.1.1. Prazo de validade, não inferior a 60 (sessenta) dias, a contar da data de sua apresentação.

9.1.2. Valor unitário de cada item cotado, expressos em moeda corrente nacional (R$), considerando as especificações constantes no anexo I.
9.1.3. Descrever detalhadamente todas as características dos itens ofertados, de acordo com as especificações contidas nos anexos deste ato convocatório.

9.2. É responsabilidade da contratada incluir todos os valores necessários para entrega do objeto, inclusive, quando for o caso, aqueles referentes a frete, embalagem, diferença de alíquota e outros.

9.3. Serão desclassificadas as propostas que não atenderem as exigências do presente ato convocatório e seus Anexos, que sejam omissas ou que apresentem irregularidades insanáveis, como fraude ou falsificação de documentos, superfaturamento de preços, conluio entre os participantes, entre outras.

9.4. É facultado ao Contratante a solicitação de amostras dos materiais cotados, no prazo máximo de 3 (três) dias úteis, contados da solicitação efetuada por este Centro, devendo ser entregues no Protocolo do Cebraspe - SAAN Quadra 01, Lotes 1095 a 1145 SAAN, Brasília - DF, 70632-100, no horário das 8h às 12h e de 14h às 18h, de segunda a sexta-feira, em dias úteis.

10. DA VIGÊNCIA DO CONTRATO

10.1. A vigência do Contrato será de 12 (doze) meses, contados da data da assinatura do Contrato, podendo ser prorrogada nos temos do Regulamento de Compras e Contratações do Cebraspe.

11. DA ASSINATURA DO INSTRUMENTO CONTRATUAL

11.1. Para a assinatura do contrato de registro de preços deverá a participantes apresentar a seguinte documentação:

11.1.1. Ato Constitutivo, Estatuto ou Contrato Social e última alteração em vigor, devidamente registrado no órgão competente;

11.1.2. Cópia do Documento de Identidade e CPF do Representante Legal da empresa.

11.1.3. Certidão Negativa de regularidade com a Fazenda Federal, mediante certidão conjunta negativa de débitos, ou positiva com efeitos de negativa, relativos aos tributos federais e à Dívida Ativa da União;

11.1.4. Certidão Negativa de regularidade com as Fazendas Estaduais e do Distrito Federal, mediante certidão conjunta negativa de débitos, ou positiva com efeitos de negativa, relativos aos tributos federais e à Dívida Ativa dos Estados e do Distrito Federal;

11.1.5. Certidão Negativa de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante Certidão Negativa de Débitos Trabalhistas, ou certidão positiva com efeitos de negativa;

11.1.6. Certidão Negativa de regularidade relativa ao Fundo de Garantia do Tempo de Serviço, mediante Certificado de Regularidade;

11.1.7. Certidão Negativa de Falência ou Concordata;

11.1.8. Declaração de que não têm participação, a qualquer título, de dirigentes ou empregados desta entidade, ou parentes destes, em linha reta ou colateral, até o terceiro grau, no Contratante;

11.1.9. Declaração de que não emprega menores de dezoito em trabalho noturno, perigoso ou insalubre, e menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir de quatorze anos.

11.2. Para fins de comprovação da capacidade técnica, ou documento similar, a empresa deverá apresentar Atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, declarando ter a empresa realizado ou estar realizando o objeto compatível em características com o objeto deste Ato convocatório.

11.2.1. O atestado, ou documento similar, deverá referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

11.2.2. O Cebraspe se reserva o direito de promover diligências para certificação da legitimidade do atestado/declaração ou documento similar apresentado, podendo exigir, entre outros documentos, a apresentação do Contrato correspondente à prestação do serviço ou notas fiscais.

11.2.3. O atestado ou documento similar deve conter o nome completo, endereço e o telefone fixo de contato do atestador, “e-mail” ou qualquer outro meio com o qual o Cebraspe possa valer-se para manter contato, se necessário.

12. DA ALTERAÇÃO CONTRATUAL

12.1. As alterações contratuais poderão ser propostas pelas partes e, sendo aceitas, serão promovidas sempre que se tenha a necessidade de atendimento de interesses deste Centro e serão formalizadas por meio de termo aditivo, nos termos do Regulamento de Compras e Contratos do Cebraspe.

13. DA VIGÊNCIA DO REGISTRO DE PREÇOS

13.1. A vigência do Registro de Preços será de 12 (doze) meses, contados da data da assinatura do Contrato, podendo ser prorrogada a interesse do Contratante, desde que a pesquisa de mercado demonstre que o preço registrado se mantém vantajoso, nos termos do Regulamento de Compras e Contratações do Cebraspe.

14 - DA INTEGRIDADE E DA CONDUTA ÉTICA

14.1. A plena execução do objeto deste contrato pressupõe, além do cumprimento das cláusulas e condições definidas neste instrumento, a observância, por parte da contratada, de procedimentos de integridade e anticorrupção e a adoção de conduta ética na execução dos serviços, atendendo integralmente ao que dispõe a Lei nº 12.846/2013, a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) e o Regulamento de Compras e Contratações do Cebraspe.

14.2. A subcontratação total ou parcial do objeto do contrato somente será permitida mediante autorização prévia e expressa do CONTRATANTE, por escrito. Nesses casos, a Contratada permanecerá integralmente responsável pela execução dos serviços, bem como pelas obrigações legais, trabalhistas, previdenciárias, fiscais e comerciais decorrentes da execução contratual, ainda que realizados por terceiros subcontratados.

14.2.1. O descumprimento desta cláusula poderá ensejar a rescisão contratual, sem prejuízo da aplicação das penalidades cabíveis.

14.2.2. Na hipótese de o Cebraspe admitir a subcontratação de parcela do objeto deste contrato, a CONTRATADA ficará obrigada a inserir esta cláusula contratual no instrumento a ser celebrado com a empresa subcontratada.

15. DA GARANTIA CONTRATUAL

15.1. As informações registradas na plataforma da contratada deverão ser sustentadas por 2 (dois) anos. Após esse período deverá permitir a exportação em formato digital utilizável pelo Cebraspe para consultas futuras.

15.2. O CEBRASPE poderá exigir da contratada a prestação de garantia de execução do contrato para assegurar o efetivo cumprimento das obrigações assumidas.

15.3. O tipo de garantia é de escolha do prestador e poderá ser realizada por meio de:
15.3.1. Caução em dinheiro;
15.3.2. Fiança bancária; ou
15.3.3. Seguro garantia.

16. DAS DISPOSIÇÕES FINAIS

16.1. O presente registro de preços não gera, por parte do Contratante, obrigação de contratação exclusiva com a Contratada, tampouco impede a contratação de outras empresas para a prestação dos mesmos ou similares serviços, conforme conveniência, oportunidade e interesse público.

16.2. A Contratante reserva-se o direito de realizar contratações diretas ou por outros meios legais, independentemente da existência deste registro de preços, sem que isso gere qualquer direito à Contratada a indenizações ou compensações de qualquer natureza.

16.3. A contratada deverá executar o fornecimento de acordo com as necessidades que lhe forem apresentadas pelo Cebraspe, mediante a entrega da Ordem de Fornecimento ou outro documento equivalente.

16.4. O CEBRASPE reserva-se ao direito de cancelar o certame seletivo antes de assinado o contrato, desde que justificado.

16.5. Fica eleito o foro de Brasília/DF para dirimir quaisquer controvérsias oriundas do presente certame seletivo, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

Núcleo de Gestão de Contratos e Fornecedores

MODELO DE APRESENTAÇÃO DA PROPOSTA COMERCIAL

Prezados Senhores,

Apresentamos a V.Sª, nossa proposta para registro de Preços para futura aquisição de Solução de Segurança de Rede com características de Next Generation Firewall (NGFW) composta por hardware e software, com serviço especializado de instalação, integração, armazenamento de logs, com licenciamento e suporte do fabricante por 36 (trinta e seis) meses para uso nas dependências do Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos (Cebraspe).

O prazo de validade de nossa proposta é de 60 (sessenta) dias corridos, contados da data de sua apresentação. Declaramos que estamos de pleno acordo com todas as condições estabelecidas no Ato convocatório e seus anexos, bem como aceitamos todas as obrigações e responsabilidades especificadas na minuta de contrato.

Caso nossa proposta seja a vencedora, comprometemo-nos a assinar o Contrato no prazo estabelecido no respectivo a seguir documento de convocação. Para esse fim, apresentamos os dados necessários para a formalização contratual:

Razão Social: _____

Código e descrição da atividade econômica principal: _____

CNPJ: _____

Endereço: _____

CEP: _____Cidade: _____ UF: ___

Tel/Fax: _____

Banco: _____ Agência: _____ nº c/c: _____
Chave PIX: _____ (aceito somente o CNPJ)

Dados do Representante Legal da Empresa para assinatura do Contrato:

Nome: _____

Endereço: _____

CEP: _____ Cidade: _____ UF: _____

CPF/MF: _____ Cargo/Função: _____

Cart. Ident nº: _____ Expedido por: _____

Naturalidade: _____ Nacionalidade: _____

Local e Data.

_____

[Nome e Assinatura do Representante da Empresa Emitente]

Cargo / CPF

(Junto com a proposta de preços, deverá ser enviada a planilha com os valores unitários e a descrição das especificações de cada item).

MODELO DE DECLARAÇÃO DE PARENTESCO

A empresa _____, doravante denominada CONTRATADA, sediada na _____, CEP: _____, inscrita no CNPJ nº _____, neste ato representada pelo (a) Senhor (a) _____, portador (a) da Carteira de Identidade nº _____e do CPF nº _____, declara para fins de participação do certame em referência, que não tem a participação, a qualquer título, de dirigentes ou empregados do Cebraspe, ou parentes destes, em linha reta ou colateral, até o terceiro grau.

MODELO DE DECLARAÇÃO DE MENOR

A empresa _____, doravante denominada CONTRATADA, sediada na _____, CEP: _____, inscrita no CNPJ nº _____, neste ato representada pelo (a) Senhor (a) _____, portador (a) da Carteira de Identidade nº _____e do CPF nº _____, declara para fins do disposto no inciso XXXIII, do art. 7º da Constituição Federal, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos,
salvo menor, a partir de 14 (quatorze) anos, na condição de aprendiz.

Local e data

_____

Nome e Assinatura do Representante Legal

PROCESSO ADMINISTRATIVO 7000000XXX

CONTRATO DE PRESTAÇÃO DE SERVIÇO Nº XX/202X

CONTRATO DE REGISTRO DE PREÇOS QUE ENTRE SI CELEBRAM O CENTRO BRASILEIRO DE PESQUISA EM AVALIAÇÃO E SELEÇÃO E DE PROMOÇÃO DE EVENTOS E A EMPRESA XXXXXXXXXXXX.

O Centro Brasileiro de Pesquisa em Avaliação e Seleção e de Promoção de Eventos (Cebraspe), com sede no Setor de Armazenamento e Abastecimento Norte – SAAN Quadra 1 Lotes 1095, 1105, 1115, 1125, 1135 e 1145, em Brasília/DF, CEP 70.632-100, associação civil de direito privado, sem fins lucrativos e substituto tributário, portanto está obrigado à retenção de tributos federais (INSS, IRRF, PIS, COFINS e CSLL) e no âmbito distrital do Imposto Sobre Serviços de Qualquer Natureza (ISSQN), incidentes sobre os serviços contratados, com base nas legislações específicas vigentes, quando couber, incumbida da pesquisa, do ensino e do desenvolvimento institucional na área da educação, inscrita no CNPJ nº 18.284.407/0001-53 e I.E. 07.667.195/001-06, doravante denominado CONTRATANTE, neste ato representado pela Diretora Geral, Senhora XXXXX, portadora da Carteira de Identidade nº XXXXX e do CPF nº XXXXX e pela Diretora Executiva, Senhora XX, portadora da Carteira de Identidade nº XXXXX e do CPF nº XXXXX e a empresa XXXXX LTDA, sediada na XXXXX, em XX/XX, CEP XXXXX, inscrita no CNPJ nº XXXXX, doravante denominada CONTRATADA, neste ato representada pelo Sr. XX, portador(a) da Carteira de Identidade nº XXXXX e do CPF nº XXXXX, firmam o presente contrato, com fundamento no Código Civil Brasileiro, no Regimento Interno e no Regulamento de Compras e Contratações do Cebraspe, aprovados pelas Resoluções nº 01, de 10 de janeiro de 2014 e nº 8 de 22 de agosto de 2018, respectivamente, do Conselho de Administração do Cebraspe, em conformidade com os termos do Ato Convocatório nº 08/2025 e as cláusulas e condições a seguir enumeradas:

CLÁUSULA PRIMEIRA - DO OBJETO

1.1. O presente Contrato tem por objeto, o Registro de Preços para futura aquisição de Solução de Segurança de Rede com características de Next Generation Firewall (NGFW) composta por hardware e software, com serviço especializado de instalação, integração, armazenamento de logs, com licenciamento e suporte do fabricante por 36 (trinta e seis) meses para uso nas dependências do Cebraspe, conforme especificações e quantidades constantes neste contrato e no Termo de Referência.

1.2. O Termo de Referência, contendo as especificações técnicas detalhadas dos equipamentos e serviços, é parte integrante deste Contrato, independentemente de transcrição.

CLÁUSULA SEGUNDA – DOS LOCAIS E PRAZOS DE ENTREGA DOS EQUIPAMENTOS

2.1. A solução de segurança de rede (NGFW), incluindo equipamentos, softwares e serviços de instalação e configuração, será instalada e disponibilizada nas dependências do Cebraspe, em Brasília/DF, em locais indicados pela Superintendência de TIC ou área técnica responsável.

2.2. O prazo para entrega dos equipamentos e para a disponibilização da solução em condições de operação será de até XX (XXXXX) dias, contados a partir da emissão da Ordem de Fornecimento.

2.3. As características técnicas mínimas dos equipamentos e dos serviços, inclusive dimensionamento, funcionalidades de firewall de próxima geração, recursos de inspeção de aplicações, VPN, alta disponibilidade, armazenamento de logs e mecanismos de suporte, constam no Anexo ao Termo de Referência.

CLÁUSULA TERCEIRA – DA VIGÊNCIA DO CONTRATO

3.1. A vigência deste Contrato será de 12 (doze) meses contados da data de sua assinatura, podendo ser prorrogado, a critério do Cebraspe, mediante aditivos, nos termos do Regulamento de Compras e Contratações do Cebraspe.

3.2. O período de suporte e licenciamento do fabricante dos equipamentos e softwares será de 36 (trinta e seis) meses, contado a partir da data de aceitação definitiva da solução, observadas as condições estabelecidas no Termo de Referência.

CLÁUSULA QUARTA DO RECEBIMENTO DOS EQUIPAMENTOS

4.1. O recebimento dos equipamentos compreenderá duas etapas distintas, a seguir discriminadas:

> 4.1.1. Provisoriamente, no prazo de até 1 (um) dia útil a partir da disponibilização do equipamento, mediante termos próprios, para efeito de posterior verificação da conformidade dos serviços com a especificação técnica constante do Anexo do Termo de Referência;
>
> 4.1.2. Definitivamente, no prazo de até 5 (cinco) dias úteis a partir da disponibilização provisória dos equipamentos, mediante atesto de nota fiscal, após a verificação da qualidade e quantidade e consequente aceitação;

4.2. Em caso de não conformidade, lavrar-se-á Termo de Recusa e Devolução, no qual se consignarão as desconformidades com as exigências, hipótese em que a solução será rejeitada, devendo a CONTRATADA proceder à substituição, correção ou refazimento dos serviços no prazo de até 10 (dez) dias, quando se realizarão novamente as verificações previstas nos subitens 4.1.1 e 4.1.2;

4.3. À CONTRATADA caberá sanar todas as irregularidades apontadas no recebimento definitivo, submetendo a etapa impugnada a nova verificação, ficando sobrestado o pagamento até a execução do saneamento necessário, sem prejuízo da aplicação das sanções cabíveis, sendo que os custos de substituição e/ou reparo correrão exclusivamente às suas expensas;

4.4. O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho dos itens fornecidos, cabendo-lhe sanar quaisquer irregularidades detectadas quando do recebimento.

CLÁUSULA QUINTA – DO VALOR

5.1. O valor estimado deste Contrato é de R$ XX.XXX,XX (XXXXXXXXX reais) para futuras aquisições, mediante solicitação da CONTRATANTE e serão considerados os preços registrados constante da Proposta de Preços apresentado pela CONTRATADA.

5.2. A composição detalhada dos valores, por item e serviço, observará a proposta vencedora do Ato Convocatório nº 08/2025, fazendo parte integrante deste Contrato.

CLÁUSULA SEXTA - DAS OBRIGAÇÕES DA CONTRATADA

6.1. A CONTRATADA deve cumprir todas as obrigações constantes neste contrato e seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

6.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste contrato e seus anexos, acompanhado da respectiva nota fiscal na qual constarão as indicações referentes a marca, fabricante, modelo, procedência e prazo de garantia ou validade;

6.3. Responsabilizar-se pelos vícios e danos decorrentes do fornecimento, quando for o caso;

6.4. Reparar, corrigir, remover, ou substituir, a suas expensas, no todo ou em parte, os itens em que se verificarem vícios, defeitos ou incorreções, resultantes de erro ou falha de execução, ficando a CONTRATANTE autorizada a descontar dos pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos, salvo quando o defeito for, comprovadamente, provocado por uso indevido.

6.5. Indicar preposto para representá-la durante a execução do contrato, quando for o caso;

6.6. Arcar com todas as despesas como transporte, taxas, impostos ou quaisquer outros acréscimos legais, que correrão por conta exclusiva da CONTRATADA no âmbito do objeto deste contrato;

6.7. Comunicar à CONTRATANTE, por escrito, qualquer anormalidade ocorrida e prestar os devidos esclarecimentos e/ou informações necessárias;

6.8. O produto contratado somente será atestado como entregue pelo Fiscal e Gestor do Contrato, ou representante indicado pela CONTRATANTE, quando efetivamente prestado pela CONTRATADA, conforme descrito na Cláusula quarta;

6.9. Em caso de fusão, cisão ou incorporação da pessoa jurídica da CONTRATADA, somente serão admitidos os efeitos contratuais desta avença com a anuência por escrito da CONTRATANTE, desde que não afetem a boa execução dos serviços;

6.10. A CONTRATADA deverá arcar integralmente com eventuais obrigações decorrentes de condenação trabalhista em ações movidas por seus empregados ou ex-empregados, inclusive aquelas em que o CONTRATANTE for condenado solidariamente ou subsidiariamente, ficando assegurado à CONTRATANTE o direito de ingressar com ação regressiva em desfavor da CONTRATADA para cobrança de danos não quitados por esta e desembolsados por aquele;

6.11. A CONTRATADA deverá arcar integralmente com todas as verbas trabalhistas devidas a seus empregados, observada a legislação em vigência bem como eventuais acordos, dissídios e/ou convenções coletivas de trabalho da respectiva categoria;

6.12. A CONTRATADA será exclusivamente responsável por prestar o devido auxílio aos trabalhadores eventualmente envolvidos em acidentes de trabalho;

6.13. A CONTRATADA deverá arcar integralmente com eventuais obrigações tributárias referentes à execução do contrato de prestação de serviços, sem qualquer acréscimo ao valor do contrato;

6.14. A CONTRATADA será exclusivamente responsável por comunicar a toda e qualquer autoridade competente os acidentes de trabalho eventualmente ocorridos com seus empregados, na prestação dos serviços contratados;

6.15. A ausência de fiscalização da CONTRATANTE não exime a CONTRATADA da total responsabilidade quanto ao cumprimento das obrigações pactuadas;

6.16. A CONTRATADA não poderá subcontratar, ceder ou transferir, o total ou parte alguma do objeto contratado salvo mediante prévia e expressa autorização da CONTRATANTE;

6.17. A CONTRATADA não poderá permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre, conforme inciso XXXIII, do art. 7º da Constituição Federal.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATANTE

7.1. Fiscalizar e acompanhar a execução da entrega dos produtos e/ou serviços;

7.2. Proporcionar todas as facilidades para que a CONTRATADA possa cumprir suas obrigações durante o horário de expediente e dentro das normas e condições previstas neste termo, incluindo o acesso às dependências da CONTRATANTE;

7.3. Rejeitar, no todo ou em parte, os produtos e/ou serviços entregues em desacordo com as especificações e obrigações assumidas pela CONTRATADA;

7.4. Notificar, por escrito (por meio de carta, e-mail, ofício, e/ou ordem de serviço), à CONTRATADA, a ocorrência de eventuais imperfeições no curso da entrega dos itens, fixando prazo para sua correção;

7.5. Promover os pagamentos dentro do prazo estipulado para tal.

7.6. O Cebraspe não responderá por quaisquer compromissos assumidos pela CONTRATADA com terceiros, ainda que vinculados à execução do objeto contratado, bem como por qualquer dano causado a terceiros em decorrência de ato da CONTRATADA, de seus empregados, prepostos ou subordinados.

CLÁUSULA OITAVA – DO ACOMPANHAMENTO E FISCALIZAÇÃO

8.1. A execução do contrato será acompanhada e fiscalizada por um representante do Cebraspe, o qual deverá atestar a nota fiscal quando comprovada a fiel e correta entrega dos itens para fins de pagamento;

8.2. A presença da fiscalização do Cebraspe não elide nem diminui a responsabilidade da CONTRATADA.

8.3. Caberá ao responsável indicado recusar, totalmente ou em parte, quaisquer produtos e/ou serviços que não estejam de acordo com as exigências, podendo ser substituído qualquer produto e/ou serviço eventualmente fora de especificação;

8.4. O Cebraspe, por intermédio de técnicos de seu quadro, promoverá o acompanhamento e a fiscalização da entrega dos produtos e/ou serviços, sob os aspectos qualitativos e quantitativos, tendo total acesso aos dados referentes ao fornecimento, podendo fazer apontamentos e solicitar medidas corretivas;

8.5. O responsável deverá promover o registro das ocorrências verificadas, adotando providências necessárias ao fiel cumprimento das cláusulas contratuais, determinando o que for necessário à regularização das faltas ou imperfeições observadas;

8.6. A conformidade dos itens contratados deverá ser verificada junto ao documento da CONTRATADA que contenha a relação detalhada deles, de acordo com o estabelecido neste contrato e seus anexos.

CLÁUSULA NONA – DOS RECURSOS ORÇAMENTÁRIOS

9.1. As despesas decorrentes desta contratação serão cobertas pelos recursos oriundos da receita obtida pelo Cebraspe no exercício das suas atividades institucionais definidas em seu Estatuto.

CLÁUSULA DÉCIMA - DO FATURAMENTO

10.1. A nota fiscal de serviço, deverá ser disponibilizada, obrigatoriamente, em extensões de arquivos de dados “PDF”, pela CONTRATADA, através de *e-mail* remetido somente ao endereço eletrônico: recebimento@cebraspe.org.br.

10.2. A CONTRATADA deverá destacar no documento eletrônico o número do Contrato, período de referência, quantidades, bem como, as especificações detalhadas do objeto do contrato.

10.3. Havendo quaisquer desconformidades em razão dos preceitos dos itens 10.1 e 10.2, o documento fiscal será devolvido para as devidas correções.

CLÁUSULA DÉCIMA PRIMEIRA - DO PAGAMENTO

11.1. O pagamento será efetuado pelo Cebraspe em favor da CONTRATADA, em até 20 (vinte) dias úteis, após o recebimento da Nota Fiscal/Fatura discriminada, desde que devidamente atestada por representante do contratante especialmente designado para acompanhar e fiscalizar a execução do contrato, mediante depósito em conta bancária, que deve ser indicada pela CONTRATADA no momento da assinatura do contrato de obrigações.

11.2. Ao Cebraspe reserva-se o direito de recusar o pagamento se, no ato da atestação, os serviços não estiverem de acordo com as especificações contidas no Contrato e seus anexos.

11.3. Nos casos de eventuais atrasos de pagamentos, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, mediante solicitação da CONTRATADA, o valor devido pelo Cebraspe será atualizado financeiramente desde a data referida no item 11.1 até a data do efetivo pagamento, incidindo, apenas e tão somente, multa moratória de 2% e juros ao mês de 1%, ambos sobre o valor total da nota fiscal em aberto.

CLÁUSULA DÉCIMA SEGUNDA – DO REAJUSTE

12.1. Os preços contratados poderão sofrer reajuste após o interregno de 1 (um) ano, a contar da celebração do presente contrato.

12.2. Quando da solicitação do reajuste, este somente será concedido mediante negociação entre as partes, considerando-se:

12.2.1. Os preços praticados no mercado;
12.2.2. As particularidades do contrato em vigência;
12.2.3. A nova planilha com a variação dos custos apresentada;
12.2.4. Indicadores setoriais, tabelas de fabricantes, valores oficiais de referência, tarifas públicas ou outros equivalentes; e
12.2.5. A disponibilidade orçamentária da **CONTRATANTE**.

12.3. A **CONTRATANTE** poderá realizar diligências para conferir a variação de custos alegada pela **CONTRATADA**.

12.4. A **CONTRATANTE** deverá assegurar-se de que os preços contratados são compatíveis com aqueles praticados no mercado, de forma a garantir a continuidade da contratação vantajosa.

12.5. A **CONTRATANTE** poderá prever o pagamento retroativo do período que a proposta de reajuste permaneceu sob sua análise, por meio de Termo de Reconhecimento de Dívida.

12.6. Na hipótese do item anterior, o período que a proposta permaneceu sob análise da **CONTRATANTE** será contado como tempo decorrido para fins de contagem da anualidade do próximo reajuste.

CLÁUSULA DÉCIMA TERCEIRA - DOS ACRÉSCIMOS E DAS SUPRESSÕES

13.1. Os valores contratados poderão ser alterados nas hipóteses de complementação, acréscimo ou supressão que se fizerem necessário, por determinação do Cebraspe, conforme disposto no Regulamento de Compras e Contratações do Cebraspe.

CLÁUSULA DÉCIMA QUARTA – DA SEGURANÇA DO TRABALHO

14.1. A CONTRATADA deverá cumprir a legislação e as normas relativas à Segurança e Medicina do Trabalho, diligenciando para que seus empregados trabalhem com Equipamentos de Proteção Individual (EPI), quando couber, e executem os testes necessários e definidos na legislação pertinente. A fiscalização da CONTRATANTE poderá paralisar os serviços, enquanto tais empregados não estiverem protegidos, ficando o ônus da paralisação por conta da CONTRATADA.

14.2. A CONTRATADA deverá observar, adotar, cumprir e fazer cumprir todas as normas de segurança e prevenção de acidentes no desempenho de cada etapa dos serviços.

CLÁUSULA DÉCIMA QUINTA – DO SIGILO

15.1. A CONTRATADA guardará e fará com que o seu pessoal e os eventuais subcontratados guardem absoluto sigilo sobre dados, informações e documentos fornecidos pela Contratante, sendo vedada toda e qualquer reprodução dos mesmos.

15.2. Todas as informações, resultados, relatórios e quaisquer outros documentos obtidos e/ou elaborados pela CONTRATADA na execução dos serviços serão de exclusiva propriedade da Contratante, não podendo a CONTRATADA utilizá-los para qualquer fim, ou divulgá-los, reproduzi-los ou veiculá-los, a não ser que prévia e expressamente autorizado pela Contratante.

15.3. A CONTRATADA fica ciente de que toda e qualquer informação, dado ou conhecimento que seus funcionários tenham acesso por força da execução do contrato configura-se como dado sigiloso, comprometendo-se a guardar o devido sigilo, sob pena de descumprimento grave, bem como das sanções penais e cíveis cabíveis, em especial pelas perdas e danos que possam vir a ser causadas em razão da revelação para terceiros de tais dados.

CLÁUSULA DÉCIMA SEXTA - DA INTEGRIDADE E DA CONDUTA ÉTICA

16.1. A plena execução do objeto deste contrato pressupõe, além do cumprimento das cláusulas e condições definidas neste instrumento, a observância, por parte da CONTRATADA, de procedimentos de integridade e anticorrupção e a adoção de conduta ética na execução dos serviços, atendendo integralmente ao que dispõe a Lei nº 12.846/2013, a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018) e o Regulamento de Compras e Contratações do Cebraspe.

16.1.1. Na hipótese de o Cebraspe admitir a subcontratação de parcela do objeto deste contrato, a CONTRATADA ficará obrigada a inserir esta cláusula contratual no instrumento a ser celebrado com a empresa subcontratada.

CLÁUSULA DÉCIMA SÉTIMA - DA RESCISÃO DAS OBRIGAÇÕES

17.1. A inexecução total ou parcial de qualquer dispositivo do presente instrumento, após prévia e ampla defesa, dará causa à sua rescisão, sem prejuízo de outras penalidades previstas neste instrumento de contrato, em obediência ao Regulamento de Compras e Contratações do Cebraspe.

17.2. O Cebraspe poderá rescindir este Contrato a qualquer momento e sem ônus, desde que a CONTRATADA seja notificada com antecedência mínima de 30 (trinta) dias.

17.3. O contrato poderá ser rescindido mediante acordo entre as partes.

CLÁUSULA DÉCIMA OITAVA – DA VIGÊNCIA DO REGISTRO DE PREÇOS

18.1. A vigência do Registro de Preços será de 12 (doze) meses a partir da data de sua assinatura, podendo ser prorrogado a critério do Cebraspe, nos termos do art. 17 do Regulamento de Compras e Contratações do Cebraspe.

CLÁUSULA DÉCIMA NONA – DO REGISTRO DE PREÇOS

19.1. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, materiais ou serviços registrados, cabendo ao Cebraspe promover as negociações junto aos fornecedores.

19.2. Quando o preço registrado se tornar superior ao preço praticado no mercado por motivo superveniente, o Cebraspe convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.

19.3. Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

19.4. O fornecedor terá seu registro cancelado de pleno direito nas seguintes hipóteses:

I) Por iniciativa do Cebraspe:

a) quando o fornecedor der causa à rescisão administrativa do Contrato decorrente do registro de preços;

b) se os preços registrados estiverem superiores aos praticados no mercado.

II) Por iniciativa do fornecedor:

a) mediante solicitação escrita, comprovando estar impossibilitado de cumprir os requisitos do Registro de Preços;

b) quando comprovada a ocorrência de descumprimento de quaisquer cláusulas contratuais pelo Cebraspe.

19.5. O cancelamento do registro de preços poderá ocorrer também por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento do Contrato, devidamente comprovados e justificados:

a) por razão de interesse do Cebraspe; ou
b) a pedido do fornecedor.

19.6. Ocorrendo cancelamento do preço registrado, o fornecedor será informado por correspondência com aviso de recebimento, a qual será juntada ao processo administrativo.

19.7. A solicitação do fornecedor para cancelamento dos preços registrados poderá não ser aceita pelo Cebraspe, facultando-se a este, neste caso, a aplicação das penalidades previstas no Contrato.

19.8. Havendo o cancelamento do preço registrado, cessarão todas as atividades do fornecedor relativas ao respectivo registro.

19.9. Caso se abstenha de aplicar a prerrogativa de cancelar o registro, o Cebraspe poderá, a seu exclusivo critério, suspender a sua execução e/ou sustar o pagamento das faturas, até que o fornecedor cumpra integralmente a condição contratual infringida.

CLÁUSULA VIGÉSIMA – DA GARANTIA DOS EQUIPAMENTOS

20.1. Os equipamentos devem possuir garantia de 60 (sessenta) meses com um período de disponibilidade para chamada de manutenção com essas características:

20.2. Atendimento remoto em até 4 horas;

20.3. Recebimento de peça essencial, depois de diagnosticado pela equipe do suporte, em até 4 horas. Peças não essenciais no próximo dia útil;

20.4. Chegada ao local de um técnico especialista no dia útil seguinte, após a identificação pelo suporte da necessidade de um técnico especialista no local;
20.5. Com suporte proativo;

20.6. Com substituição proativa;

20.7. Com atualização de software e firmware vinculados aos equipamentos e drivers;
20.8.Com monitoramento remoto em período integral (24x7);

20.9. Com 4 horas de serviço de montagem da atualização e configuração pelos técnicos do fabricante;

20.10. A CONTRATANTE poderá abrir chamados de manutenção diretamente no fabricante do item sem necessidade de prévia consulta e/ou qualquer liberação por parte da CONTRATADA. Não deve haver limite para aberturas de chamados, sejam de dúvidas/configurações e/ou resolução de problemas de hardware ou software;

20.11. A abertura de chamados poderá ser realizada através de telefone 0800 do fabricante, através da página da WEB do fabricante ou através de endereço de e-mail do fabricante;

20.12. A abertura de chamados através de telefone 0800 deverá ser realizada inicialmente em português;

20.13. Deverá ser garantido à CONTRATANTE o pleno acesso ao site do fabricante dos equipamentos e softwares. Esse acesso deve permitir consultas a quaisquer bases de dados disponíveis para usuários relacionadas aos equipamentos e softwares especificados, além de permitir downloads de quaisquer atualizações de software ou documentação deste produto.

20.14. Durante o período de garantia, devem ser disponibilizados e instalados, sem ônus à CONTRATANTE, todas as atualizações de software e firmware para os equipamentos, quando for necessário;

20.15. A CONTRATADA deve apresentar os códigos/sku's/part number do serviço de garantia do fabricante dos equipamentos, sendo que todos os equipamentos deverão ser previamente registrados pelo fornecedor junto ao fabricante, em nome da CONTRATANTE.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO FORNECIMENTO

21.1. A presente contratação não importa direito subjetivo do contratado de exigir o fornecimento exclusivo nas quantidades indicadas neste instrumento, sendo facultada ao Cebraspe a realização de contratações de terceiros sempre que houver preços mais vantajosos, em obediência expressa ao Regulamento de Compras e Contratações do Cebraspe.

21.2. A CONTRATADA deverá executar o fornecimento/serviço de acordo com as necessidades que lhe forem apresentadas pelo Cebraspe, mediante a entrega da Ordem de Fornecimento ou outro documento equivalente.

CLÁUSULA VIGÉSIMA SEGUNDA – DAS CLÁUSULAS PENAIS

22.1. Advertência.

22.2. Multa de 10% (dez por cento) sobre o valor total da Ordem de Fornecimento, no caso de inexecução parcial ou total da obrigação assumida;

22.3. Suspensão temporária do direito de contratar com o Cebraspe, pelo prazo de até 2 (dois) anos, nos casos de inadimplemento das obrigações assumidas;
22.4. O valor da multa, aplicada após a regular notificação da CONTRATADA e transcorrido o prazo de 5 (cinco) dias para defesa, será cobrado por meio da emissão de duplicata, em que o Cebraspe, constará como credor, ou cobrado judicialmente;

22.5. As multas e outras sanções aplicadas só poderão ser relevadas, motivadamente e por conveniência do Cebraspe, mediante Resolução do Diretor-Geral (RDG), devidamente justificada;

22.6. As sanções de advertência e de impedimento de contratar com o Cebraspe poderão ser aplicadas juntamente com a multa;

22.7. As cláusulas penais são convencionadas e serão aplicadas de acordo com os artigos 408 a 416 do Código Civil;

22.8. As sanções previstas nesta cláusula também serão aplicadas às empresas ou aos profissionais que, em razão dos contratos regidos pelo Regulamento de Compras e Contratações do Cebraspe:

22.8.1 Apresentem documentação falsa;
22.8.2 Cometam fraude na execução deste contrato;
22.8.3 Comportem-se de modo inidôneo;
22.8.4 Tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;
22.8.5 Tenham praticado atos ilícitos visando a frustrar os objetivos da contratação;
22.8.6 Utilizem meio imoral ou antiético nos relacionamentos com os empregados do CONTRATANTE;
22.8.7 Recusem-se a cooperar com o Cebraspe, em caso de denúncia, suspeita de irregularidade ou de violação da Lei nº 12.846/2013 relativas à execução do presente contrato.

CLÁUSULA VIGÉSIMA TERCEIRA - DAS DISPOSIÇÕES GERAIS

23.1. Fica vedada na execução deste Contrato a participação, a qualquer título, de dirigentes ou empregados do Cebraspe, ou parentes destes, em linha reta ou colateral até o terceiro grau.

23.2. Fazem parte integrante deste Contrato, o Termo de Referência, o Edital do Ato Convocatório nº 08/2025 e seus anexos, a proposta comercial e os elementos que a acompanham.
23.3. Fica eleito o Foro da cidade de Brasília/DF para dirimir questões relativas ao presente contrato, com exclusão de qualquer outro.

23.4. E, para firmeza e prova de assim haverem, entre si, ajustado e acordado, após ter sido lido, o presente contrato é assinado eletronicamente pelas partes.

CONTRATANTE:_____
ADRIANA RIGON WESKA

CONTRATANTE:_____
CLAUDIA MAFFINI GRIBOSKI

CONTRATADA:_____
XXXXXXXXXXXX

TERMO DE REFERÊNCIA

1. DO OBJETO

1.1. O presente termo de referência tem por objeto a aquisição de Solução de Segurança de Rede com características de Next Generation Firewall (NGFW) composta por hardware e software, com serviço especializado de instalação, integração, armazenamento de logs, com licenciamento e suporte do fabricante por 36 (trinta e seis) meses para uso nas dependências do Cebraspe.

2. DO FUNDAMENTO LEGAL

2.1. A contratação do objeto deste Termo de Referência encontra amparo legal nas normas constantes no Código Civil Brasileiro, no Regimento Interno e no Regulamento de Compras e Contratações do Cebraspe, aprovados pelas Resoluções nº 1, de 10 de janeiro de 2014 e nº 8 de 22 de agosto de 2018, respectivamente, do Conselho de Administração do Cebraspe.

3. DAS CARACTERÍSTICAS DOS SERVIÇOS

3.1. A descrição completa dos equipamentos e dos serviços a serem adquiridos encontra-se no anexo do presente termo de referência.

4. DO RECEBIMENTO DOS SERVIÇOS

4.1. O recebimento dos serviços compreenderá duas etapas distintas, a seguir discriminadas:

4.1.1. Provisoriamente, no prazo de até 1 (um) dia útil a partir da disponibilização do serviço, mediante termos próprios, para efeito de posterior verificação da conformidade dos serviços com a especificação prevista neste contrato;

4.1.2. Definitivamente, no prazo de até 5 (cinco) dias úteis a partir da disponibilização provisória dos canais, mediante atesto de nota fiscal, após a verificação da qualidade e quantidade dos serviços e consequente aceitação;

4.2. Em caso de não conformidade, lavrar-se-á Termo de Recusa e Devolução, no qual se consignarão as desconformidades com as exigências. Nessa hipótese, o serviço objeto deste termo será rejeitado, devendo ser substituído ou refeito no prazo de 10 (dez) dias, quando se realizarão novamente as verificações em conformidade com os itens 4.1.1 e 4.1.2;

4.3. À CONTRATADA caberá sanar as irregularidades apontadas no recebimento definitivo, submetendo a etapa impugnada a nova verificação, ficando sobrestado o pagamento até a execução do saneamento necessário, sem prejuízo da aplicação das sanções cabíveis, sendo que os custos da substituição e/ou reparo dos serviços rejeitados correrão exclusivamente a expensas da CONTRATADA;

4.4. O recebimento não exclui a responsabilidade da CONTRATADA pelo perfeito desempenho dos serviços fornecidos, cabendo-lhe sanar quaisquer irregularidades detectadas quando do recebimento.

5. DAS OBRIGAÇÕES DA CONTRATADA

5.1. A CONTRATADA deve cumprir todas as obrigações constantes neste Termo de Referência e no contrato, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

5.2. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes neste Termo de Referência e no Contrato, acompanhado da respectiva nota fiscal;

5.3. Responsabilizar-se pelos vícios e danos decorrentes do serviço fornecido;

5.4. Reparar, corrigir, remover, ou substituir, a suas expensas, no todo ou em parte, os serviços em que se verificarem vícios, defeitos ou incorreções, resultantes de erro ou falha de execução, ficando a CONTRATANTE autorizada a descontar dos

pagamentos devidos à CONTRATADA, o valor correspondente aos danos sofridos, salvo quando o defeito for, comprovadamente, provocado por uso indevido;

5.5. Indicar preposto para representá-la durante a execução do contrato, quando for o caso;

5.6. Arcar com todas as despesas como transporte, taxas, impostos ou quaisquer outros acréscimos legais, que correrão por conta exclusiva da CONTRATADA no âmbito desta prestação de serviços;

5.7. Comunicar à CONTRATANTE, por escrito, qualquer anormalidade ocorrida e prestar os devidos esclarecimentos e/ou informações necessárias;

5.8. O serviço contratado somente será atestado como entregue pelo Fiscal e Gestor do Contrato, ou representante indicado pela CONTRATANTE, quando efetivamente prestado pela CONTRATADA;

5.9. A CONTRATADA deverá arcar integralmente com eventuais obrigações decorrentes de condenação trabalhista em ações movidas por seus empregados ou ex-empregados, inclusive aquelas em que o CONTRATANTE for condenado solidariamente ou subsidiariamente, ficando assegurado à CONTRATANTE o direito de ingressar com ação regressiva em desfavor da CONTRATADA para cobrança de danos não quitados por esta e desembolsados por aquele;

5.10. A CONTRATADA deverá arcar integralmente com todas as verbas trabalhistas devidas a seus empregados, observada a legislação em vigência bem como eventuais acordos, dissídios e/ou convenções coletivas de trabalho da respectiva categoria;

5.11. A CONTRATADA será exclusivamente responsável por prestar o devido auxílio aos trabalhadores eventualmente envolvidos em acidentes de trabalho;

5.12. A CONTRATADA deverá arcar integralmente com eventuais obrigações tributárias referentes à execução do contrato de prestação de serviços, sem qualquer acréscimo ao valor do contrato;

5.13. A CONTRATADA será exclusivamente responsável por comunicar a toda e qualquer autoridade competente os acidentes de trabalho eventualmente ocorridos com seus empregados, na prestação dos serviços contratados;

5.14. A ausência de fiscalização da CONTRATANTE não exime a CONTRATADA da total responsabilidade quanto ao cumprimento das obrigações pactuadas;

5.15. A CONTRATADA não poderá subcontratar, ceder ou transferir, o total ou parte alguma do objeto contratado;

5.16. Em caso de fusão, cisão ou incorporação da pessoa jurídica da CONTRATADA, somente serão admitidos os efeitos contratuais desta avença com a anuência por escrito da CONTRATANTE, desde que não afetem a boa execução dos serviços;

5.17. A CONTRATADA não poderá permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre, conforme inciso XXXIII, do art. 7º da Constituição Federal.

6. DAS OBRIGAÇÕES DA CONTRATANTE

6.1. Fiscalizar e acompanhar a execução da entrega dos serviços;

6.2. Proporcionar todas as facilidades para que a contratada possa cumprir suas obrigações durante o horário de expediente e dentro das normas e condições previstas neste termo, incluindo o acesso às dependências da CONTRATANTE;

6.3. Rejeitar, no todo ou em parte, os serviços entregues em desacordo com as especificações e obrigações assumidas pela CONTRATADA;

6.4. Notificar, por escrito (por meio de carta, e-mail, ofício, e/ou ordem de serviço), à contratada, a ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para sua correção;

6.5. Promover os pagamentos dentro do prazo estipulado para tal.

7. DO ACOMPANHAMENTO E FISCALIZAÇÃO

7.1. A execução do serviço e do contrato será acompanhada e fiscalizada por um representante do Cebraspe, o qual deverá atestar a nota fiscal quando comprovada a fiel e correta entrega dos serviços para fins de pagamento;
7.2. A presença ou não da fiscalização do Cebraspe não elide nem diminui a responsabilidade da CONTRATADA;
7.3. Caberá ao responsável indicado recusar, totalmente ou em parte, quaisquer serviços que não estejam de acordo com as exigências, podendo ser substituído qualquer serviço eventualmente fora de especificação;
7.4. O Cebraspe, por intermédio de técnicos de seu quadro, promoverá o acompanhamento e a fiscalização da entrega dos serviços prestados, sob os aspectos qualitativos e quantitativos, tendo total acesso aos dados referentes ao fornecimento, podendo fazer apontamentos e solicitar medidas corretivas;
7.5. O responsável deverá promover o registro das ocorrências verificadas, adotando providências necessárias ao fiel cumprimento das cláusulas contratuais, determinando o que for necessário à regularização das faltas ou imperfeições observadas;
7.6. A conformidade dos serviços contratados deverá ser verificada junto ao documento da CONTRATADA que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste termo e seus anexos.

8. DO CONTRATO

8.1. A vigência do Contrato será de 12 (doze) meses a partir da data de sua assinatura, podendo ser prorrogado a critério do Cebraspe, nos termos do parágrafo 1º do art. 26 do Regulamento de Compras e Contratações do Cebraspe.

9. DOS RECURSOS

9.1. As despesas decorrentes desta contratação serão cobertas pelos recursos oriundos da receita obtida pelo Cebraspe no exercício das suas atividades institucionais definidas em seu Estatuto.

10. DO FATURAMENTOO

10.1. Os documentos fiscais deverão ser disponibilizados, obrigatoriamente, em extensões de arquivos de dados “PDF” e “XML”, pela Contratada, através de e-mail remetido somente ao endereço eletrônico: recebimento@cebraspe.org.br ;
10.2. A Contratada deverá destacar no documento eletrônico o número do Contrato, período de referência, quantidades, bem como, as especificações detalhadas do objeto do contrato;
10.3. Havendo quaisquer desconformidades em razão dos preceitos dos itens 10.1 e 10.2, o documento fiscal será devolvido para as devidas correções.

11. DO PAGAMENTO

11.1. O pagamento será efetuado mensalmente pelo Cebraspe em favor da CONTRATADA em até 10 (dez) dias úteis após o recebimento da nota fiscal/fatura discriminada, desde que devidamente atestada pelo representante do CONTRATANTE especialmente designado para acompanhar e fiscalizar a execução do contrato, mediante depósito em conta bancária, que deve ser indicada pela CONTRATADA no momento da assinatura do contrato;
11.2. Ao Cebraspe reserva-se o direito de recusar o pagamento se, no ato da atestação, os serviços não estiverem de acordo com as especificações contidas neste termo;
11.3. Nos casos de eventuais atrasos de pagamentos, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, mediante solicitação da CONTRATADA, o valor devido pelo Cebraspe será atualizado financeiramente desde a data referida no item 11.1 até a data do efetivo pagamento, incidindo, apenas e tão somente, multa moratória de 2% e juros ao mês de 1%, ambos sobre o valor total da nota fiscal em aberto.

12. DOS ACRÉSCIMOS E SUPRESSÕES

12.1. Os valores contratados poderão ser alterados nas hipóteses de complementação, acréscimo ou supressão que se fizerem necessário, por determinação do Cebraspe, conforme disposto no Regulamento de Compras e Contratações do Cebraspe.

13. DA SEGURANÇA DO TRABALHO

13.1. A CONTRATADA deverá obedecer às normas de segurança do trabalho aplicáveis aos seus empregados, de acordo com a Legislação Vigente, especialmente o fornecimento do equipamento de proteção individual (EPI), quando for o caso, bem como a exigência e fiscalização quanto ao uso do material, não sendo cabível qualquer responsabilização da CONTRATATANTE em caso de acidentes de trabalho.

14. DO SIGILO

14.1. A CONTRATADA guardará e fará com que os seus empregados e os eventuais subcontratados guardem absoluto sigilo sobre dados, informações e documentos fornecidos pela CONTRATATANTE, sendo vedada toda e qualquer reprodução;

14.2. Todas as informações, resultados, relatórios e quaisquer outros documentos obtidos e/ou elaborados pela CONTRATADA na execução dos serviços serão de exclusiva propriedade da CONTRATATANTE, não podendo a CONTRATADA utilizá-los para qualquer fim, ou divulgá-los, reproduzi-los ou veiculá-los, a não ser que prévia e expressamente autorizado pela CONTRATATANTE;

14.3. A CONTRATADA fica ciente de que toda e qualquer informação, dado ou conhecimento que seus funcionários tenham acesso por força da execução deste contrato configura-se como sigiloso, e se compromete a guardar o devido sigilo, sob pena de descumprimento grave, bem como de aplicação das sanções cíveis e penais cabíveis, em especial pelas perdas e danos que possam vir a ser causadas em razão da revelação para terceiros de tal informação, dado ou conhecimento.

15. DA INTEGRIDADE E DA CONDUTA ÉTICA

15.1. A plena execução do objeto deste contrato pressupõe, além do cumprimento das cláusulas e condições definidas neste instrumento, a observância, por parte da CONTRATADA, de procedimentos de integridade e anticorrupção e a adoção de conduta ética na execução dos serviços, atendendo integralmente ao que dispõe a Lei nº 12.846/2013 e o Regulamento de Compras e Contratações do Cebraspe.

15.2. Na hipótese de o Cebraspe admitir a subcontratação de parcela do objeto deste contrato, a contratada ficará obrigada a inserir esta cláusula contratual no instrumento a ser celebrado com a empresa subcontratada.

16. DA RESCISÃO DAS OBRIGAÇÕES

16.1. A inexecução total ou parcial de qualquer dispositivo do presente instrumento convocatório e no contrato a ser entabulado, após prévia e ampla defesa, dará causa à rescisão do contrato, sem prejuízo de outras penalidades previstas nos referidos instrumentos, em obediência ao art. 32 do Regulamento de Compras e Contratações do Cebraspe;

16.2. O Cebraspe poderá rescindir o contrato a qualquer momento e sem ônus, desde que a contratada seja notificada com antecedência mínima de 30 (trinta) dias.

17. DA GARANTIA

17.1. As informações registradas na plataforma da contratada deverão ser sustentadas por 2 (dois) anos. Após esse período deverá permitir a exportação em formato digital utilizável pelo Cebraspe para consultas futuras.

18. DO CRONOGRAMA

18.1. Cada entrega será realizada com uma reunião de alinhamento para prevenção de retrabalhos e correções de possíveis análises que possam ter sido levantadas com alguma diferença.

19. DAS CLÁUSULAS PENAIS

19.1. Advertência.

19.2. Multa de:

19.2.1. 0,3% (três décimos por cento) ao dia sobre o valor contratado, no caso de atraso injustificado na execução do objeto, limitada a incidência a 15 (quinze) dias;

19.2.2. 0,5% (cinco décimos por cento) ao dia sobre o valor contratado, no caso de atraso injustificado na execução do objeto por período superior a 15 (quinze) dias, limitado a 30 (trinta) dias. Após o trigésimo-primeiro dia e a critério do Cebraspe, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença;

19.2.3. 10% (dez por cento) sobre o valor total da Ordem de Fornecimento, no caso de inexecução parcial superior a 30 (trinta) dias, ou no caso de inexecução total da obrigação assumida;

19.3. Suspensão temporária do direito de contratar com o Cebraspe, pelo prazo de até 2 (dois) anos, nos casos de inadimplemento das obrigações assumidas;

19.4. O valor da multa, aplicada após a regular notificação da contratada e transcorrido o prazo de 5 (cinco) dias para defesa, será cobrado por meio da emissão de duplicata, em que o Cebraspe, constará como credor, ou cobrado judicialmente;

19.5. As multas e outras sanções aplicadas só poderão ser relevadas, motivadamente e por conveniência do Cebraspe, mediante Resolução do Diretor-Geral (RDG), devidamente justificada;

19.6. As sanções de advertência e de impedimento de contratar com o Cebraspe poderão ser aplicadas juntamente com a multa;

19.7. As cláusulas penais são convencionadas e serão aplicadas de acordo com os artigos 408 a 416 do Código Civil;

19.8. As sanções previstas nesta cláusula também serão aplicadas às empresas ou aos profissionais que, em razão dos contratos regidos pelo Regulamento de Compras e Contratações do Cebraspe:

19.8.1. Apresentem documentação falsa;

19.8.2. Cometam fraude na execução deste contrato;

19.8.3. Comportem-se de modo inidôneo;

19.8.4. Tenham sofrido condenação definitiva por praticarem, por meios dolosos, fraude fiscal no recolhimento de quaisquer tributos;

19.8.5. Tenham praticado atos ilícitos visando a frustrar os objetivos da contratação;

19.8.6. Utilizem maio imoral ou antiético nos relacionamentos com os empregados do contratante;

19.8.7. Recusem-se a cooperar com o Cebraspe, em caso de denúncia, suspeita de irregularidade ou de violação da Lei nº 12.846/2013 relativas à execução do presente contrato.

ANEXO I
Especificações Técnicas Mínimas

Item 1 – Firewall
Quantidade: 2 Firewalls

1. CARACTERÍSTICAS GERAIS

1.1. A solução deverá ser composta de hardware e software licenciado, do mesmo fabricante;
1.2. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;
1.3. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;
1.4. 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;

1.5. Todos os componentes devem ser próprios para montagem em rack "19" e deverão ser fornecidos pela Contratada, incluindo kit tipo trilho para adaptação, cabos de alimentação, suportes, gavetas e braços, se necessário;

1.6. Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e v3;

1.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipamentos distintos;

2. NGFW - CAPACIDADE E QUANTIDADES

2.1. ITEM 1 - SOLUÇÃO EM APPLIANCE DE SEGURANÇA DE PERÍMETRO DE PRÓXIMA GERAÇÃO

2.1.1. Deve suportar operação em cluster ativo-ativo sem a necessidade de licenças adicionais.
2.1.2. A unidade da solução contratada deve operar em cluster e ter as seguintes capacidades:
2.1.3. Throughput de, no mínimo, 6,5 (seis vírgula cinco) Gbps, quando ativadas simultaneamente as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, Anti-Bot e prevenção de ameaças avançadas de dia zero;
2.1.4. Suporte a, no mínimo, 16 M (dezesseis milhões) de conexões simultâneas;
2.1.5. Suporte a, no mínimo, 250.000 (duzentos e cinquenta mil) novas conexões por segundo;
2.1.6. Throughput de, no mínimo, 26 (vinte e seis) Gbps, no mínimo, para conexões VPN;
2.1.7. Suportar, no mínimo, a criação de 20 instâncias/contextos virtuais de firewall;

2.1.8. Deve suportar a performance considerando as funcionalidades de Next Generation firewall de 18 (dezoito) Gbps;
2.1.9. Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;
2.1.10. Fonte de alimentação redundante;
2.1.11. Throughput de no mínimo, 28 (vinte e oito) Gbps de IPS;
2.1.12. Deve possuir no mínimo 32 (trinta e dois) GB de memória RAM;
2.1.13. No mínimo, 04 (quatro) interfaces de rede 10/25Gbps SFP28;
2.1.14. No mínimo, 08 (oito) interfaces de rede 10/100/1000 Base-T;
2.1.15. Possuir 1 (uma) interface de rede dedicada para sincronismo;
2.1.16. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;
2.1.17. Possuir 1 (uma) interface do tipo console ou similar;
2.1.18. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.
2.1.19. Os equipamentos devem possuir arquitetura modular de interfaces de rede, permitindo a substituição de interfaces por outras com tipo de conexão e velocidades diferentes;
2.1.20. Cada um dos appliances da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) com no mínimo 480 GB de capacidade de armazenamento para o Sistema Operacional.
2.1.21. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.1.22. Suporte a RFC 4291 de Arquitetura de endereçamento IPv6.
2.1.23. Solução de suportar Dual stack ipv4/ipv6 e NAT64.
2.1.24. Suportar configurar IPv6 em Dual Stack em uma interface Bond/Agregação, essa configuração também pode ser configurada em uma Sub-interface de Bond/Agregação;
2.1.25. Deve suportar NAT64 e NAT46;
2.1.26. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
2.1.27. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos e regras;
2.1.28. Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;
2.1.29. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

2.1.30. Os valores de capacidade são considerados para cada equipamento, não sendo permitido a soma dos valores dos membros do cluster;

2.1.31. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores. Caso sejam fornecido hardware adicional para compor a solução de alta disponibilidade e balanceamento de carga, esta deve possuir no mínimo 08 interfaces de 40/100G QSFP+. Caso não exista elemento externo, essas interfaces devem ser fornecidas no próprio appliance NGFW.

3. **FUNCIONALIDADES DE ALTA DISPONIBILIDADE E BALANCEAMENTO DE CARGA**

3.1. Permitir a configuração dos appliances em modo de alta disponibilidade, com suporte mínimo aos seguintes modos de configuração: Ativo-Ativo.

3.2. A alternância entre os dispositivos configurados em modo de alta disponibilidade deve se dar no mínimo pelos seguintes parâmetros de detecção de anomalia:

3.2.1. Falha de funcionamento do dispositivo.

3.2.2. Falha de link, seja por falha no tráfego (path monitoring) quanto por falha de alguma das suas interfaces (Interface Monitoring).

3.3. Deverá ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino, que deverá estar comunicável através da rota. Caso haja falha na comunicação, o firewall deverá ter a capacidade de usar alternativa para restabelecer a comunicação.

3.4. Operando em alta disponibilidade, os dispositivos deverão, no mínimo, sincronizar as seguintes informações entre si:

3.4.1. Certificados digitais, informações registradas em sua Forwarding Information Base(FIB), configurações registradas em suas políticas de firewall incluindo em seus objetos de rede, configurações de NAT e possuir administração através de linha de comando através de SSH versão 2 e através de interface WEB.

3.5. A solução de balanceamento deve possuir a capacidade de, automaticamente, por meio de definições de *thresholds*, executar a realocação de tráfego entre os equipamentos que compõem o cluster, ou o redirecionamento do tráfego sem a necessidade de intervenção física para este redirecionamento.

3.6. Deve ser possível configurar segmentação lógica do tráfego entre os membros do cluster, de forma que um ou mais appliances sejam reservados para tratar determinado de tipo de tráfego (tráfego local, por exemplo), e outro(s) membro(s) sejam reservados para tratar outro tipo de tráfego (tráfego destinado para a nuvem, por exemplo).

3.7. A solução deve ser capaz de ser gerenciada através de um único endereço IP para todo o cluster, de forma que todos os appliances que componham o cluster tenham um gerenciamento unificado.

3.8. A solução deve permitir o uso de diferentes modelos de appliance no cluster, de forma a flexibilizar o crescimento da plataforma no futuro sem a necessidade da aquisição de um cluster de igual capacidade;

4. **FUNCIONALIDADE DE FIREWALL**

4.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;
4.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;
4.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;
4.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;
4.5. Realizar upgrade via SCP, SFTP e https via interface WEB
4.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:
  4.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;
  4.6.2. Deverá suportar VXLAN;
4.7. Deve suportar os seguintes tipos de NAT:
  4.7.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;
4.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
4.9. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;
4.10. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizáveis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Objetos dinâmicos que não se caracterizam como FQDN.
4.11. Enviar logs para sistemas de monitoração externos, simultaneamente;
4.12. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;
4.13. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância (contexto) de firewall.
4.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
4.15. Suportar OSPF graceful restart;
4.16. Deve suportar roteamento ECMP (equal cost multi-path);
4.17. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâmetros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

4.18. Autenticação integrada via Kerberos.

4.19. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.

4.20. As regras Firewall devem suportar "hit count" para monitorar a quantidade de conexões que deram matches em cada regra;

4.21. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

4.22. A solução deve ter a capacidade de operar através de uma única instancia de Firewall de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

4.23. A solução deve permitir salvar as configurações das políticas para serem aplicadas em horários pré-definidos;

4.24. Deve possuir mecanismo de ativação de validada da regra com período customizado;

4.25. Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet.

4.26. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento.

4.27. Deve permitir a configuração do tempo de checagem para cada um dos links.

5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

5.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

5.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

5.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

5.3.1. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

5.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

5.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

5.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

5.5.2. Reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

5.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;
5.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)
5.8. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;
5.8.1. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;
5.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;
5.10. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 100 categorias de aplicações WEB pré-definidas pelo fabricante;
5.11. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);
5.12. Possui mecanismo de controle de aplicação web e URL que possui configuração de bloqueio e liberação da aplicação principal e/ou as suas subcategorias. Quando o administrador da solução desejar bloquear apenas as subcategorias do facebook, como facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também pode implicar o bloqueio não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote.
5.13. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;
5.14. Atualizar a base de assinaturas de aplicações automaticamente;
5.15. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;
5.16. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;
5.17. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;
5.18. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;
5.19. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;
5.20. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

5.20.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

5.20.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

5.20.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

5.20.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

5.20.5. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

5.20.6. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção "Safe Search" esteja desabilitada no navegador do usuário;

5.20.7. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

5.20.8. Suportar a criação de categorias de URLs customizadas;

5.20.9. Suportar a exclusão de URLs do bloqueio, por categoria;

5.20.10. Permitir a customização de página de bloqueio;

5.21. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

5.22. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

5.23. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

6. FUNCIONALIDADE DE FILTRO DE DADOS

6.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

6.1.1. • PCI - credit card numbers

6.1.2. • HIPAA - Medical Records Number - MRN

6.1.3. • International Bank Account Numbers - IBAN

6.1.4. • Source Code - JAVA

6.1.5. • U.S. Social Security Numbers - According to SSA

6.1.6. • Salary Survey Terms

6.1.7. • Viewer File - PDF

6.1.8. • Executable file

6.1.9. • Database file

6.1.10. • Document file

6.1.11. • Presentation file

6.1.12. • Spreadsheet file

6.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

6.3. A solução de controle de dados deve permitir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito.

6.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

7. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

7.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

7.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

7.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

7.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

7.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

7.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

7.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

7.7. Detectar e bloquear a origem de portscans;
7.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;
7.9. Possuir assinaturas para bloqueio de ataques de buffer overflow;
7.10. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;
7.11. Suportar bloqueio de arquivos por tipo;
7.12. Identificar e bloquear comunicação com botnets;
7.13. Deve suportar referência cruzada com CVE;
7.14. Em cada proteção de segurança, deve estar incluso informações como:
    7.14.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro código de referência;
    7.14.2. Severidade.
    7.14.3. Tipo de ação a ser executada.
7.15. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.
7.16. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.
7.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.
7.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)
7.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
    7.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;
7.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;
7.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;
7.22. A solução de IPS deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações que aponta quais das assinaturas que estão em modo detecção deve ser alteradas para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.
7.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;
7.24. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;
7.25. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.
7.26. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

7.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;
7.28. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;
7.29. A solução de IPS deve possuir engine onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;
7.30. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.
7.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso
7.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;
7.33. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;
7.34. A solução deve permitir a criação de White list baseado no MD5 do arquivo;
7.35. Os eventos devem identificar o país de onde partiu a ameaça;
7.36. A funcionalidade de IPS e anti-bot, deve possuir capacidade de correlacionar em seus logs a visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;
7.37. Suportar rastreamento de vírus em arquivos pdf;
7.38. Deve suportar a inspeção em arquivos comprimidos (zip, gzip, etc.);
7.39. Possuir a capacidade de prevenção de ameaças não conhecidas;
7.40. Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueada
7.41. A solução de Antivírus e Anti-Malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);
7.42. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;
7.43. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;
7.44. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
7.45. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS do tipo DGA (Domain Genaration Algorithm) não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

7.46. A solução deverá possuir mecanismo de "machine learning" para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

7.47. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo Firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

7.48. A solução de Anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

7.49. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & Control);

7.50. A solução Antivírus deverá suportar a análise de links no corpo de e-mails.

8. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

8.1. Suportar a criação de políticas de QoS por:

8.2. Endereço de origem, endereço de destino e por porta;

8.3. O QoS deve possibilitar a definição de classes por:

8.4. Banda garantida, banda máxima e fila de prioridade;

8.5. Disponibilizar estatísticas em tempo real para classes de QoS;

8.6. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE (Private or Public APN) e Satélite.

8.7. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

8.8. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

8.9. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo

8.10. Deve permitir a comunicação indireta entre localidades por meio de uma topologia "hub and spoke"

8.11. Deve balancear o tráfego de aplicativos em vários links simultaneamente

8.12. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas

8.13. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamente fora dos túneis via underlay.

8.14. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço

8.15. Suportar políticas inteligentes usando configuração padrão de fábrica que executem redirecionamento automático e imposição de QoS de voz, vídeo e tráfego transacional

8.16. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo

8.17. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo.

8.18. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

8.19. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação de políticas em grande escala.

8.20. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional.

8.21. Usar probes artificiais baseadas em icmp, udp ou tcp para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latência e perda de pacotes.

8.22. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade.

8.23. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar.

8.24. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

8.25. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

8.26. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver congestionamento em pontos remotos

8.27. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

8.28. O console de gerenciamento deve informar o status operacional (UP/DOWN/SPEED) das interfaces LAN e WAN

8.29. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade

8.30. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

8.31. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

8.32. No caso do Orchestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução.

9. FUNCIONALIDADES DE VPN

9.1. Suportar VPN Site-to-Site e Cliente-To-Site;

9.2. Suportar IPSec VPN;

9.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

9.4. Suportar SSL VPN;

9.5. A VPN IPSEc deve suportar:

9.5.1. 3DES, Autenticação MD5, SHA-1, AES-XCBC, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

9.6. A VPN SSL deve suportar:

9.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

9.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

9.6.3. Suportar configuração de conformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

9.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

9.6.5. Atribuição de DNS nos clientes remotos de VPN;

9.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

9.6.7. A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus, firewall no host, chaves de registros e processos ativos;

9.6.8. A solução deve permitir bloquear o acesso dos usuários aos recursos via VPN caso o usuário não esteja em conformidade com a verificação dos parâmetros configurados.

9.6.9. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

9.6.10. A solução deve permitir a integração da ferramenta com provedores de identidade, através de SAML, para autenticação dos usuários remotos conectados via VPN;

9.6.11. Suportar leitura e verificação de CRL (certificate revocation list);

9.6.12. A tecnologia de VPN Client to Server deverá ser compatível na plataforma: iOS 10 ou superior e Android;

9.6.13. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 10, Windows 11 e MacOS X;

10. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY

10.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

10.2. Não serão aceitas soluções que dependam da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

10.3. A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.

10.4. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA durante

análise completa do arquivo no ambiente sandbox, sem que o arquivo seja entregue parcialmente ao cliente.

10.5. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

10.6. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

10.7. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

10.8. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

10.9. O conteúdo enviado 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;

10.10. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

10.11. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem. Não serão aceitas soluções em servidores ou software livre;

10.12. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

10.13. Toda análise deverá ser realizada em nuvem do próprio fabricante, não sendo aceitas soluções que necessitem de módulos e/ou servidores externos para a implementação de máquinas virtuais;

10.14. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

10.15. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

10.16. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

10.17. A solução deve suportar inspeção para o protocolo SMBv3;

10.18. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

10.19. A solução deve possuir engine de inspeção a nível de CPU para detectar técnicas ROP (Return Of Operation) além de outras técnicas de exploração de vulnerabilidade monitorando o fluxo de CPU;

10.20. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a

necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

10.21. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

10.22. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

10.23. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

10.24. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

10.25. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

10.26. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

10.27. A solução deve permitir bloquear o acesso do usuário caso este tente fazer o envio de suas informações em sites classificados como phishing;

10.28. O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

10.29. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

10.29.1. Número de arquivos emulados;

10.29.2. Número de arquivos com malware.

10.30. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outra solução de mercado, não sendo ela soluções abertas;

10.31. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

10.31.1. O tamanho máximo do arquivo emulado seja excedido;

10.31.2. O tempo máximo de emulação seja excedido.

11. MÓDULO DE GERÊNCIA

11.1. A solução de gerência poderá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;

11.2. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado a maior capacidade suportada ou ilimitada;

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

11.4. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;

11.5. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

11.6. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

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

11.8. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

11.9. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

11.10. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

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

11.12. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

11.13. Suportar backup das configurações e rollback de configuração para a última configuração salva;

11.14. Suportar validação de regras antes da aplicação;

11.15. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

11.16. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;

11.17. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

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

11.19. Permitir a criação de certificados digitais para autenticação de usuários;

11.20. O relatório deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos GW's de segurança, sendo que deve possuir relatório e telas de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-Malware e Sandboxing);

11.21. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.

11.22. A solução deve permitir a integração da ferramenta com provedores de identidade para autenticação dos administradores da solução via SAML 2.0;

11.23. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

11.23.1. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com no mínimo, os perfis de aprovador e solicitante.

11.23.2. A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes formas, Email, Requisição WEB ou Scripts.

11.24. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

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

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

11.27. Deve ser possível exportar os logs em CSV ou TXT;

11.28. A solução deve ser capaz de segmentar a base de regras em uma estrutura em camadas;

11.29. A solução deve ser capaz de aplicar proteções relacionadas a ameaças e regras de acesso separadamente;

11.30. A solução deve combinar configuração de políticas e análise de logs em um único painel, para evitar erros alcançando maior confiabilidade na alteração de políticas;

11.31. O visualizador de log deve ter um recurso de pesquisa de texto livre;

11.32. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

11.33. Possibilitar rotação do log;

11.34. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

11.34.1. 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 um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

11.35. Deve permitir a criação de relatórios personalizados;

11.36. O gerenciamento centralizado poderá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESX (vSphere 5.1 ou superior), HYPER-V, ou outro virtualizador de mercado;

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

11.38. Possuir capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI.

11.39. Deve consolidar logs e relatórios de todos os dispositivos administrados;

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

11.41. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;
11.42. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;
11.43. A gerência centralizada deve possuir modulo de solução para validação de conformidade de acordo com normas de mercado conforme exemplo.
  11.43.1. ISO 27001 e ISO 27002;
  11.43.2. PCI-DSS;
  11.43.3. NIST 800-41
  11.43.4. GDPR (base da norma LGPD);
11.44. A solução para validação de conformidade, deve ser contemplada para o primeiro ano de projeto para adequação as novas normas de mercado que a instituição irá seguir. Não sendo permitido licenciamento mensalizado “trial”, ou seja, deve ser considerado uma licença de uso anual, podendo ela ser renovada por um período maior.
11.45. Caso a solução não possua tal modulo, será permitido composição com soluções de mercado, não sendo elas soluções abertas “Software Livre”.
11.46. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;
11.47. Permitir a customização do padrão regulatório da própria instituição;
11.48. Permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;
11.49. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;
11.50. Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual;
11.51. Gerar alertas de conformidade notificando os usuários sobre o impacto de suas decisões de segurança trazendo as considerações regulatórias na gestão de segurança;
11.52. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;
11.53. Possuir alertas de políticas e as potenciais violações de conformidade;
11.54. Possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança;
11.55. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;
11.56. Os itens 10.43 a 10.55 se aplicam ao cluster central localizado na Sede;
11.57. Permitir que os relatórios possam ser salvos, enviados e impressos;
11.58. Deve permitir a criação de filtros 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;
11.59. A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:
  11.59.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

11.59.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

11.60. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

11.61. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

11.62. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto, gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

11.63. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

11.64. Criar certificados digitais para acesso dos usuários VPN;

11.65. Criar certificados digitais para VPNs Site-to-Site;

11.66. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;

11.67. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

11.68. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.

11.69. A plataforma de gerência centralizada e monitoração deve 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 possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivirus e navegação web simultaneamente na mesma query de pesquisa.

11.70. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

11.71. A A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes Pps e redes nos campos de origem e destino dos logs na mesma tela de pesquisa.

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

11.73. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

11.74. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

11.75. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

11.76. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

11.77. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

11.78. A solução deve ser capaz de personalizar e criar regras de correlação;

11.79. A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;
11.80. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;
11.81. A solução poderá possuir agente de Inteligência Artificial Generativa embarcado na console de gerenciamento para auxílio na redução do tempo de execução de tarefas administrativas comuns da solução, como consulta de logs relacionados à sites, arquivos ou usuários específicos;
11.82. O assistente de IA Generativa deve ser capaz de trazer informações relacionadas a logs, gerenciamento de políticas e de objetos e documentação técnica da solução para facilitar a administração da solução de firewall;
11.83. O assistente de IA Generativa deve ser capaz de trazer respostas completas e contextualizadas, interagindo com as políticas, logs e objetos para tal;
11.84. A solução de gerenciamento deve ser capaz de realizar auditoria das políticas implementadas de forma automatizada, identificando se determinada política está violando as melhores práticas pré-determinadas pela organização e alertando o administrador em caso de violação;
11.85. A solução de gerenciamento deve possuir mecanismo que identifique políticas de segurança redundantes, sem uso, ou conflitantes com políticas existentes;

12. **CARACTERÍSTICAS GERAIS**

12.1. Durante a vigência do contrato e da garantia deverão ser disponibilizadas até 3 (três) vagas anuais, para participação em eventos de capacitação técnica (nacionais ou internacionais), sem custo adicional para o Cebraspe, para atualização de conhecimentos nas tecnologias em uso;
12.2. Entende-se por eventos de capacitação técnica: Workshops, Seminários, Fóruns, Feiras Tecnológicas, Visitas técnicas e/ou Treinamento em Fabricas, Datacenters e/ou Laboratórios do fabricante/fornecedor, entre outros com o mesmo propósito.