CONSELHO FEDERAL DE ENFERMAGEM – COFEN
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

EDITAL DE PREGÃO ELETRÔNICO SRP
N°. 17/2017
PAD Nº 40/2015

O **Conselho Federal de Enfermagem – Cofen**, entidade fiscalizadora do exercício profissional *ex vi* da Lei nº. 5.905, de 12/07/1973, com sede no SCLN 304, Bloco E, Lote 9, Asa Norte, Brasília/DF, CEP: 70.736-550, CNPJ nº. 47.217.146/0001-57, e este Pregoeiro, designado pela Portaria Cofen nº. 57, de 16 de janeiro de 2017, tornam público, na forma da Lei nº. 10.520, de 17/07/2002, do Decreto nº 5.450/2005, do Decreto nº 7.892/2013, da Lei Complementar n.º 123/2006 e, subsidiariamente da Lei n.º 8.666/1993, que se acha aberta licitação na modalidade **PREGÃO ELETRÔNICO - SRP**, do tipo **MENOR VALOR POR LOTE**, em regime de execução indireta, por empreitada e por preço unitário, mediante as condições estabelecidas neste Edital, constante do PAD Cofen nº. 40/2015.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

DATA DA REALIZAÇÃO: 10/07/2017
HORÁRIO: 9:40 hs (horário de Brasília/DF)
ENDEREÇO ELETRÔNICO: www.comprasnet.gov.br
CÓDIGO UASG: 389320

I. DO OBJETO

1.1. Este edital tem por objeto o registro de preços para a aquisição por meio de **Sistema de Registro de Preços (SRP)**, de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o COFEN, compreendendo o fornecimento, a instalação, o suporte técnico, a garantia, o treinamento, o gerenciamento e o monitoramento de sistemas de: Firewall de Nova Geração (NGFW), Access Point Wireless, Switch PoE, Patch panel, Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web - WAF (Web Application Firewall), Centro de Operações de Segurança da Informação - SOC (Security Operation Center), Teste de Intrusão/Penetração (Pentest), Endpoint, Gestão Contínua de Vulnerabilidades e assinaturas conforme especificações constantes no Termo de Referência (Anexo I deste Edital).
1.2. Em caso de discordância entre as especificações deste objeto descritas no Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

II. DOS VALORES ESTIMADOS DA LICITAÇÃO

2.1 A despesa com a aquisição objeto desta licitação está estimada em **R$ 8.434.642,53** (oito milhões e quatrocentos e trinta e quatro mil e seiscentos e quarenta e dois reais e cinquenta e três centavos), conforme planilhas constantes do Termo de Referência, anexo I deste instrumento.

3. DA PARTICIPAÇÃO

3.1**.** Poderão participar deste Pregão os interessados que:
a) tenham objeto social pertinente e compatível com o objeto licitado;
b) estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores -

SICAF e perante o sistema eletrônico provido pela Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI), por meio do sítio www.comprasnet.gov.br.

3.2**.** Para ter acesso ao sistema eletrônico, os interessados em participar deste Pregão deverão dispor de chave de identificação e senha pessoal, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento e regulamento e receber instruções detalhadas para sua correta utilização.

3.3**.** O uso da senha de acesso pela licitante é de sua responsabilidade exclusiva, incluindo qualquer transação por ela efetuada diretamente, ou por seu representante, não cabendo ao provedor do sistema ou ao Cofen responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

3.4. Não poderão participar deste Pregão:

a) empresário suspenso de participar de licitação e impedido de contratar com o Conselho Federal de Enfermagem, durante o prazo da sanção aplicada;

b) empresário declarado inidôneo para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

c) empresário impedido de licitar e contratar com a União, durante o prazo da sanção aplicada;

d) empresário proibido de contratar com o Poder Público, em razão do disposto no art.72, § 8º, V, da Lei nº 9.605/98;

e) empresário proibido de contratar com o Poder Público, nos termos do art. 12 da Lei nº 8.429/92;

f) quaisquer interessados enquadrados nas vedações previstas no art. 9º da Lei nº 8.666/93;

f.1) Entende-se por "participação indireta" a que alude o art. 9º da Lei nº 8.666/93 a participação no certame de empresa em que uma das pessoas listadas no mencionado dispositivo legal figure como sócia, pouco importando o seu conhecimento técnico acerca do objeto da licitação ou mesmo a atuação no processo licitatório.

g) sociedade estrangeira não autorizada a funcionar no País;

h) empresário cujo estatuto ou contrato social não seja pertinente e compatível com o objeto deste Pregão;

i) empresário que se encontre em processo de dissolução, recuperação judicial, recuperação extrajudicial, falência, concordata, fusão, cisão, ou incorporação;

j) 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;

k) Não será admitida a participação de consórcio de empresas por inexistirem demanda que justifique a aglutinação de competências conexas que apresentem suas especificidades, o que justificaria a união de empresas, pois a Contratada deve ter apenas competência a ser comprovada por meio de atestado (s) de capacidade técnica, para executar o objeto licitado;

l) Empresários que tenham em seu quadro dirigente ou empregado do Sistema Cofen/Conselhos Regionais de Enfermagem, bem como ex-empregados, até 6 (seis) meses após a sua demissão;

m) Não será permitida a participação de cooperativas, pois o serviço a ser executado apresenta características incompatíveis com a organização do trabalho nesta modalidade, tais como:

a). Mecanismos de comando e controle visando assegurar a adoção de métodos e padrões que serão rotineiramente cobrados;

b). Relação de hierarquia técnica e funcional entre os profissionais;

c). Níveis diferenciados de responsabilização técnica.

4. DO REGISTRO DE PREÇOS

4.1**.** O Conselho Federal de Enfermagem – Cofen será o Órgão Gerenciador, sendo, portanto, o responsável pela condução da licitação e gerenciamento da Ata de Registro de Preços.

4.2. Os Conselhos Regionais de Enfermagem – Coren's, relacionados no item 2 acima, são Órgãos Participantes, conforme previsto no artigo 6º, do Decreto nº. 7892/2013;

4.3. A Ata de Registro de Preços terá validade de 12 (doze) meses, contados a partir da data de sua assinatura, com eficácia após sua publicação no Diário Oficial.

4.4. A Ata de Registro de Preços terá efeito de compromisso de fornecimento, ficando os fornecedores nela incluídos obrigados a celebrar as ordens de fornecimento ou contratos que advierem nas condições estabelecidas neste edital.

4.5. A adesão ao registro de preços decorrente do presente edital, esta restrita aos Conselhos regionais de Enfermagem, os quais fazem parte do Sistema Cofen/Corens.

4.6 As aquisições ou contratações adicionais decorrentes da adesão à Ata de Registro de Preços não poderão exceder, por Conselho Regional, a cem por cento dos quantitativos dos itens registrados na Ata de Registro de Preços para o órgão gerenciador e órgãos participantes.

4.7 Homologado o resultado deste Pregão, a licitante mais bem classificada será convocada para assinar a Ata de Registro de Preços, no prazo de até 3 (tres) dias úteis, contado da data do recebimento do documento oficial de convocação.

4.7.1. O prazo para que a licitante mais bem classificada compareça após ser convocada, poderá ser prorrogado, uma única vez, por igual período, desde que ocorra motivo justificado e aceito pelo Conselho Federal de Enfermagem.

4.7.2 É facultado ao Conselho Federal de Enfermagem, quando a convocada não assinar a Ata de Registro de Preços no prazo e condições estabelecidos, convocar as licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo, nos termos do art. 4º, inciso XXIII, da Lei 10.520/02.

4.8. Publicada na Imprensa Oficial, a Ata de Registro de Preços implicará compromisso de fornecimento nas condições estabelecidas, conforme disposto no artigo 14 do Decreto n.º 7.892/2013.

4.9. A existência de preços registrados não obriga a Administração a contratar, facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

4.10. O prazo de validade improrrogável da Ata de Registro de Preços será de no máximo 12 (doze) meses, contado da data da sua assinatura, excluído o dia do começo e incluído o do vencimento.

4.11. Durante a vigência da Ata, os preços registrados serão fixos e irreajustáveis, exceto nas hipóteses decorrentes e devidamente comprovadas das situações previstas na alínea "d" do inciso II do art. 65 da Lei nº 8.666/1993 ou no artigo 17 do Decreto n.º 7.892/2013.

4.11.1 Nessa hipótese, o Conselho Federal de Enfermagem, por razão de interesse público, poderá optar por cancelar a Ata e iniciar outro processo licitatório.

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

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

4.13. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

4.13.1. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

4.13.2. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

4.14 Não havendo êxito nas negociações previstas na Condição anterior, o órgão gerenciador deverá proceder à revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

4.15 O registro do fornecedor será cancelado quando:

4.15.1 descumprir as condições da Ata de Registro de Preços;

4.15.2. não assinar o contrato ou retirar a nota de empenho no prazo estabelecido pela Administração, sem justificativa aceitável;

4.15.3. não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

4.15.4. sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da Lei n.º 8.666, de 1993, ou no art. 7º da Lei n.º 10.520, de 2002.

4.16 O cancelamento do registro de preços nas hipóteses previstas no item 4.15.1, 4.15.2 e 4.15.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

4.17 O cancelamento do registro de preços poderá ocorrer por fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da Ata, devidamente comprovados e justificados:

4.17.1 por razão de interesse público; ou

4.17.2 a pedido do fornecedor.

4.18 Em qualquer das hipóteses anteriores que impliquem a alteração da Ata registrada, concluídos os procedimentos de ajuste, o Conselho Federal de Enfermagem fará o devido apostilamento da Ata de Registro de Preços e informará aos fornecedores registrados a nova ordem de classificação.

4.19 A Ata de Registro de Preços, decorrente desta licitação, será cancelada, automaticamente, por decurso do prazo de sua vigência.

5 - FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

5.1 - Após homologado o resultado deste Pregão, o COFEN convocará o primeiro fornecedor classificado, obedecida à ordem de classificação e aos quantitativos propostos, para assinatura da Ata de Registro de Preços, dentro do prazo de 5 (cinco) dias úteis, a partir da data da convocação.

5.2 – O COFEN convocará formalmente o fornecedor, informando o local, data e hora para a assinatura da Ata de Registro de Preços.

5.2.1 - O prazo de convocação do fornecedor poderá ser prorrogado uma única vez, por igual período, desde que ocorra motivo justificado e aceito pelo COFEN.

5.2.2 - Será incluído, na respectiva ata na forma de anexo, o registro dos licitantes que aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor na sequência da classificação do certame, excluído o percentual referente à margem de preferência, quando o objeto não atender aos requisitos previstos no art. 3º da Lei nº 8.666, de 1993;

5.3 – É facultado ao COFEN, quando o convocado não assinar a ata de registro de preços no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado.

5.3.1 – A convocação dos licitantes remanescentes de que trata o item 5.3 estará condicionada à apresentação dos documentos previstos neste edital, conforme § 3º do Art. 11 do Decreto nº 7.892/13.

5.3.2 – Nos termos do parágrafo 3º do artigo 11 do Decreto nº. 7.892/13, a habilitação dos fornecedores que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação de fornecedor remanescente, nas hipóteses previstas nos artigos 20 e 21 do Decreto nº. 7.892/13;

5.4 - Publicada na Imprensa Oficial a Ata de Registro de Preços terá efeito de compromisso de fornecimento nas condições estabelecidas, conforme o artigo 14 do Decreto n.º 7.892/2013.

6 – REGULAMENTO OPERACIONAL DO CERTAME

6.1 – Credenciamento:

6.1.1 - Para acesso ao sistema eletrônico, os interessados em participar do pregão deverão dispor de chave de identificação e senha pessoal e intransferível, no site www.comprasgovernamentais.gov.br (Art. 3º, § 1º do Decreto nº 5.450/2005).

6.1.2 - Os licitantes ou seus representantes legais deverão estar previamente credenciados perante o provedor do sistema eletrônico.
6.1.3 - O credenciamento do licitante dependerá de registro cadastral atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF.
6.1.4 - O credenciamento junto ao provedor do sistema implica a responsabilidade legal do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.
6.1.5 - O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao COFEN, promotora da licitação, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros (Art. 3º, § 5º do Decreto nº 5.450/2005).
6.1.6 - A perda da senha ou a quebra de sigilo deverão ser comunicadas imediatamente ao provedor do sistema para imediato bloqueio de acesso.
6.2. - A participação no pregão eletrônico dar-se-á por meio de conexão ao sistema eletrônico COMPRASNET, bem como pela digitação da senha pessoal e intransferível do representante credenciado e subsequente encaminhamento da proposta de preços, exclusivamente por meio eletrônico, observados data e horário limite estabelecidos.
6.2.1 - Como requisito para participação no pregão, o licitante deverá manifestar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do instrumento convocatório.
6.2.2 - A declaração falsa relativa ao cumprimento dos requisitos de habilitação e proposta sujeitará o licitante às sanções previstas no art. 28 do Decreto nº 5.450, de 31 de maio de 2005, e na legislação pertinente.
6.2.3 - O licitante será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances.
6.2.4 - Caberá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou, ainda, em razão de desconexão.

6.3 – Recebimento das Propostas:

6.3.1 - O licitante deverá observar as datas e horários limites previstos para entrega e abertura da proposta, atentando também para a data e horário para início da disputa.
6.3.2 - Todas as referências de tempo no Edital, no Aviso e durante a sessão pública observarão obrigatoriamente o horário de Brasília – DF e, dessa forma, serão registrados no sistema eletrônico e na documentação relativa ao certame.
6.3.3 - O licitante no momento da elaboração e envio de sua proposta, deverá enviar, obrigatoriamente, através de campo próprio do Sistema, as declarações de inexistência de fato superveniente e de que o mesmo não emprega menor, as quais somente serão visualizadas pelo pregoeiro na fase de habilitação, quando também poderão ser alteradas ou reenviadas pelos fornecedores, por solicitação do pregoeiro.
6.3.4 - As microempresas e empresas de pequeno porte, no ato de envio de sua proposta, em campo próprio do Sistema, deverão declarar que atendem aos requisitos do artigo 3º da Lei Complementar nº 123, de 14 de dezembro de 2006, para fazer jus aos benefícios previstos na referida Lei.
6.3.4.1 - A não entrega da Declaração indicará que a microempresa, ou empresa de pequeno porte, optou por não utilizar os benefícios previstos na Lei Complementar nº 123/2006.
6.3.5 - O licitante deverá encaminhar sua PROPOSTA DE PREÇOS preenchendo o campo específico no COMPRASNET.
6.3.5 1 A licitante deverá anexar em campo específico do COMPRASNET a PLANILHA DE PREÇOS atualizada.

6.3.5.2 - As especificações constantes da PLANILHA DE PREÇOS que não estejam de acordo com o especificado no Anexo I do Edital – Termo de Referência levarão à desclassificação do licitante.
6.3.6 - O preenchimento da proposta, bem como a inclusão de seus anexos, no sistema COMPRASNET, é de exclusiva responsabilidade do licitante, não cabendo ao COFEN qualquer responsabilidade.
6.3.7 - Até a data e hora definidas para abertura das propostas, o licitante poderá retirar ou substituir a proposta anteriormente apresentada.
6.3.8 - O pregoeiro verificará as propostas apresentadas, desclassificando aquelas que não estejam de acordo com os requisitos estabelecidos no Edital.
6.3.8.1 - Constatada a existência de proposta(s) manifestamente inexequível (eis), esta(s) será(ão) desclassificada(s) pelo pregoeiro, ficando o(s) respectivo(s) licitante(s) impedido(s) de participar da etapa de lances.
6.3.9 - A desclassificação da proposta será sempre fundamentada e registrada no sistema, podendo os participantes acompanhar o resultado da análise em tempo real.
6.3.10 - As propostas classificadas pelo pregoeiro serão ordenadas pelo sistema, automaticamente, e só estas participarão da etapa de lances.
6.4 - Sessão de disputa:
6.4.1 - No horário previsto no Edital o pregoeiro dará início à fase competitiva quando, então, os licitantes poderão encaminhar seus lances exclusivamente por meio do sistema eletrônico.
6.4.2 - Se por algum motivo a sessão de disputa não puder ser realizada na data e horário previstos, os participantes deverão ficar atentos à nova data e horário que serão disponibilizados no endereço eletrônico www.comprasgovernamentais.gov.br, opção “informações do pregão”.
6.4.3 - Os lances deverão ser formulados sobre o preço total global do grupo único, conforme Planilha de Preços – Anexo II.
6.4.4 - Os lances serão registrados no sistema, de forma sucessiva, em valores distintos e decrescentes.
6.4.5 - Cada licitante será imediatamente informado do recebimento do seu lance e do valor consignado no registro.
6.4.6 - Será permitido ao licitante oferecer lance superior ao menor lance registrado no sistema, desde que inferior ao último por ele ofertado e diferente de qualquer lance válido.
6.4.7 – Não serão aceitos mais de um lance de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
6.4.8 - Não poderá haver desistência dos lances ofertados, sujeitando-se o licitante desistente às penalidades previstas no item 14 deste Edital.
6.4.9 - Durante o transcurso da sessão, os participantes serão informados, em tempo real, do valor do menor lance registrado. O sistema não identificará o autor dos lances aos demais licitantes.
6.4.10 - Durante a fase de lances, o pregoeiro poderá excluir, justificadamente, lance cujo valor for considerado inexequível.
6.4.11 - No caso de desconexão do pregoeiro, no decorrer da etapa competitiva, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances. O pregoeiro, assim que possível, dará continuidade à sua atuação no certame, sem prejuízo dos atos realizados.
6.4.12 - Quando a desconexão do pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa e terá reinício somente após comunicação expressa do pregoeiro aos participantes.
6.4.13 - A etapa de lances será encerrada mediante aviso de fechamento iminente, emitido pelo pregoeiro aos licitantes, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a recepção de lances.
6.4.14 - Após a fase de lances, se a proposta mais bem classificada não tiver sido ofertada por microempresa ou empresa de pequeno porte e houver proposta apresentada por microempresa ou

empresa de pequeno porte, será assegurado, como critério de desempate, preferência de contratação para as microempresas e empresas de pequeno porte, conforme disposto na Lei Complementar 123/06.
6.4.14.1 - Entende-se por empate aquelas situações em que as propostas apresentadas pelas microempresas e empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores ao melhor preço.
6.4.14.2 - Para efeito do disposto na condição anterior, ocorrendo o empate, proceder-se-á da seguinte forma:
a) A microempresa ou empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos, contado do envio da mensagem automática pelo sistema, apresentar uma última oferta, obrigatoriamente, abaixo da primeira colocada, situação em que, atendidas as exigências habilitatórias, será adjudicado em seu favor o objeto deste Pregão.
b) Não sendo vencedora a microempresa ou empresa de pequeno porte mais bem classificada, na forma da subcondição anterior, o sistema, de forma automática, convocará os licitantes remanescentes que porventura se encontrem na situação descrita nesta condição, na ordem classificatória para o exercício do mesmo direito.
c) No caso de equivalência dos valores apresentados pelas microempresas ou empresas de pequeno porte que se encontrem na hipótese descrita nessa condição, o sistema fará o sorteio eletrônico, definindo e convocando automaticamente, a vencedora para o encaminhamento da oferta final do desempate.
6.4.14.3 - Na hipótese da não contratação nos termos previstos nesta seção, o objeto licitado será adjudicado em favor da proposta originalmente vencedora do certame.
6.4.14.4 - O disposto nesta seção somente se aplicará quando a melhor oferta inicial não tiver sido apresentada por microempresa ou empresa de pequeno porte.

6.5 - Procedimentos posteriores à sessão de disputa
6.5.1 - O pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para contratação.
6.5.1.1 - O pregoeiro poderá encaminhar contraproposta ao licitante que tenha apresentado lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento, não se admitindo negociar condições diferentes daquelas previstas no Edital.
6.5.1.2 - A negociação será realizada por meio do sistema eletrônico, podendo ser acompanhada pelos demais licitantes.
6.5.2 - O pregoeiro poderá anunciar o licitante vencedor imediatamente após o encerramento da etapa de lances da sessão pública ou, quando for o caso, após a negociação e decisão acerca da aceitação do lance de menor valor.
6.5.3 – Após o encerramento da etapa competitiva, os licitantes poderão reduzir seus preços ao valor da proposta do licitante mais bem classificado, sendo os mesmos, observado o disposto no item 5 deste Edital, registrados na ata de realização da sessão pública do pregão.

7 - APRESENTAÇÃO DA PROPOSTA E DOCUMENTAÇÃO

7.1 - Encerrada a etapa de lances, se a proposta de preços for aceitável, o licitante, provisoriamente detentor da melhor oferta, encaminhará:
7.1.1 - No prazo máximo de 120 (cento e vinte) minutos, contado da solicitação do pregoeiro no sistema eletrônico, os documentos de habilitação previstos neste edital e a proposta final, conforme descrito no anexo I, do termo de referencia, com os preços adequados ao seu último valor ofertado;
7.1.2 - No prazo máximo de 2 (dois) dias, os documentos enviados na forma do item 7.1.1, em originais ou cópias autenticadas, contados da solicitação do pregoeiro no sistema eletrônico.

7.1.2.1 - É de responsabilidade do licitante confirmar junto ao COFEN o recebimento dos documentos de habilitação e proposta final, não cabendo ao COFEN a responsabilidade pelo desconhecimento de tais informações.
7.1.2.2 - A proposta e demais documentos deverão ser entregues no endereço abaixo, em envelope contendo na parte externa, além da denominação social do licitante, a referência ao pregão:

CONSELHO FEDERAL DE ENFERMAGEM - COFEN
SCLN 304, Bloco E, Lote 9 - Asa Norte - CEP.: 70.736-550 - Brasília - DF
Ref.: PREGÃO ELETRÔNICO Nº 17/2017 – SRP

7.1.3 - os prazos referidos nos itens 7.1.1 e 7.1.2 poderão ser prorrogados por decisão fundamentada do pregoeiro, após análise de justificativa apresentada pelo licitante.

8 - CRITÉRIO DE JULGAMENTO DAS PROPOSTAS
8.1 - No julgamento da habilitação e das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.
8.1.1 – O pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do COFEN ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão.
8.2 - Somente será aceita proposta que contemple integralmente o grupo objeto deste Edital.
8.3 - Será desclassificada a proposta que deixar de contemplar a totalidade dos itens pertinentes ao grupo.
8.4 - Serão desclassificadas as propostas que apresentarem preços manifestamente inexequíveis, preços que sejam considerados excessivos comparativamente com os correntes de mercado, ou que apresentarem preços superiores aos preços máximos aceitos pelo COFEN, conforme Anexo V – Planilha de Preços Máximos.
8.5 - As propostas serão avaliadas pelo critério de MENOR PREÇO, levando-se em conta o preço global, constante na PROPOSTA DE PREÇOS, apresentado pelo licitante e as condições estabelecidas neste Edital.
8.6 - Em caso de divergência entre os preços unitários, subtotais, totais e global, prevalecerão os valores unitários para efeito de cálculo dos valores subtotais, totais e global.
8.7 - Os licitantes poderão vir a ser chamados pelo pregoeiro para demonstrar a exequibilidade de suas propostas.
8.8 - Não sendo aceitável a proposta ou o lance de menor preço, ou ainda, caso o licitante não atenda às exigências para habilitação, o pregoeiro examinará a proposta ou o lance subsequente, verificando a sua aceitabilidade e procedendo a sua habilitação, caso atendidos todos os requisitos, na ordem de classificação, e assim sucessivamente, até a apuração de uma proposta ou lance que atenda ao Edital.
8.9 - Ocorrendo a situação referida no subitem anterior, o pregoeiro poderá negociar com o licitante para que seja obtido preço melhor.
8.10 - Constatado o atendimento das exigências fixadas no Edital, o licitante será declarado vencedor, sendo-lhe adjudicado o objeto do certame.
8.11 – O licitante que abandonar o certame, deixando de enviar a documentação conforme indicação nos itens 7.1.1 ou 7.1.2, será desclassificado e sujeitar-se-á às sanções previstas neste edital.

9 - CONTEÚDO DA PROPOSTA
9.1 - A proposta de preços deverá conter os seguintes dados:

a) Preços unitários e totais de cada grupo, bem como o valor global, referidos à data prevista para realização da sessão pública, expressos em reais, conforme PLANILHA DE PREÇOS contida no Anexo I do termo de referencia.

a.1) Com o objetivo de facilitar o preenchimento dos valores dos itens, será disponibilizado, no sítio www.cofen.gov.br, o arquivo eletrônico da PLANILHA DE PREÇOS em extensão .xls.

b) Prazo de validade da proposta, que não deverá ser inferior a 60 (sessenta) dias, contados da data prevista para abertura deste pregão, podendo vir a ser prorrogado mediante solicitação do COFEN e aceitação do licitante.

c) No preço deverão estar inclusos todos os custos e despesas, tais como: custos diretos e indiretos, tributos, encargos sociais, trabalhistas e previdenciários, seguros, taxas, lucro embalagens, transporte e outros necessários ao cumprimento integral do objeto, sendo vedada a cobrança adicional de valores referentes a taxas de administração ou quaisquer outras despesas.

d) Razão social, endereço, telefone/fax, número do CNPJ, banco, agência, conta-corrente e praça de pagamento, nome, assinatura e telefone do representante da empresa.

9.2 - Não serão admitidos valores cotados acima dos Preços Máximos Unitários estipulados no Anexo I do termo de referencia – Planilha de Preços Máximos, sob pena de desclassificação.

X. DA HABILITAÇÃO

10.1 A habilitação das licitantes será verificada por meio do Sicaf (habilitação parcial) e da documentação complementar especificada neste Edital.

10.2 As licitantes que não atenderem às exigências de habilitação parcial no Sicaf deverão apresentar documentos que supram tais exigências.

10.3 Realizada a habilitação parcial no Sicaf, será verificado eventual descumprimento das vedações elencadas no item 3 - Da Participação na Licitação, mediante consulta ao:

a) Sicaf, a fim de verificar a composição societária das empresas e certificar eventual participação indireta que ofenda ao art. 9º, III, da Lei nº 8.666/93;

b) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça – CNJ, no endereço eletrônico www.cnj.jus.br/improbidade_adm/consultar_requerido.php;

c) Cadastro Nacional das Empresas Inidôneas e Suspensas – CEIS, no endereço eletrônico www.portaldatransparencia.gov.br/ceis.

d) Cadastro de Inidôneos e Cadastro de Inabilitados (TCU), no endereço eletrônico: https://contas.tcu.gov.br/ords/f?p=1498:3

10.4 As consultas previstas na Condição anterior realizar-se-ão em nome da sociedade empresária licitante e também de eventual matriz ou filial e de seu sócio majoritário.

10.5 Efetuada a verificação referente ao cumprimento das condições de participação no certame, a habilitação das licitantes será realizada mediante a apresentação da seguinte documentação complementar:

10.5. Certidão negativa de débitos trabalhistas (CNDT).

10.6. Ao menos um (1) atestado de capacidade técnica expedido por pessoa jurídica de direito público ou privado, em nome da licitante que comprove:

a) aptidão para desempenho de atividade pertinente e compatível em características e quantidades com o objeto desta licitação, demonstrando que a licitante executa ou executou contrato correspondente a 50% (cinquenta por cento) do valor estimado para a presente licitação;

b) Será aceito o somatório de atestados ou declarações para comprovar a capacidade técnica, desde que reste demonstrada a execução concomitante dos serviços.

10.7. Comprovação de capital social ou patrimônio líquido correspondente a 10% (dez por cento) do valor da contratação, na forma dos §§ 2° e 3° do artigo 31 da Lei 8.666/93. A comprovação será

exigida somente no caso do proponente apresentar resultado inferior a 01 (um) nos índices de Liquidez Geral, Liquidez Corrente e Solvência Geral, obtidos no SICAF.

10.9 O Pregoeiro poderá consultar sítios oficiais de órgãos e entidades emissores de certidões, para verificar as condições de habilitação das licitantes.

10.10 Os documentos que não estejam contemplados no Sicaf deverão ser remetidos em conjunto com a proposta de preços, em arquivo único, por meio da opção "Enviar Anexo" do sistema Comprasnet, no mesmo prazo estipulado.

a) Os documentos remetidos por meio da opção "Enviar Anexo" do sistema Comprasnet poderão ser solicitados em original ou por cópia autenticada a qualquer momento, em prazo a ser estabelecido pelo Pregoeiro.

b) Os originais ou cópias autenticadas, caso sejam solicitados, deverão ser encaminhados ao Conselho Federal de Enfermagem, para o endereço descrito no rodapé deste edital.

c) Sob pena de inabilitação, os documentos encaminhados deverão estar em nome da licitante, com indicação do número de inscrição no CNPJ.

e) Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz, e a licitante comprovar a centralização do recolhimento de contribuições na matriz, quando então todos os documentos deverão estar em nome desta;

f) Em se tratando de microempresa ou empresa de pequeno porte, havendo alguma restrição na comprovação de regularidade fiscal, será assegurado o prazo de 5 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que a proponente for declarada vencedora do certame, prorrogáveis por igual período, a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do débito, emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

g) A não regularização da documentação, no prazo previsto na condição anterior, implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste Edital, e facultará ao Pregoeiro convocar as licitantes remanescentes, na ordem de classificação.

10.11 Se a proposta não for aceitável, ou se a licitante não atender às exigências de habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este Edital.

10.12 Constatado o atendimento às exigências fixadas neste Edital, a licitante será declarada vencedora.

XI. DO RECURSO ADMINISTRATIVO

11.1. Declarado o vencedor, qualquer licitante poderá, durante a sessão pública, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recorrer, quando lhe será concedido o prazo de 3 (três) dias para apresentar as razões do recurso, ficando os demais licitantes, desde logo, intimados para, querendo, apresentarem contrarrazões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

11.2. A ausência de manifestação imediata e motivada pelo licitante quanto à intenção de recorrer no prazo fixado pelo pregoeiro importará na decadência deste direito, ficando o pregoeiro autorizado a adjudicar o objeto ao licitante vencedor.

11.3. O recurso contra decisão do pregoeiro não terá efeito suspensivo.

11.4. Na ausência de recursos ou após decididos os recursos eventualmente interpostos, será adjudicado o objeto do certame ao licitante declarado vencedor, estando o resultado final da licitação sujeito à homologação pela autoridade superior competente.

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

11.6. Os recursos contra a decisão do pregoeiro, quando interpostos, deverão ser registrados, exclusivamente, no sistema Comprasnet em campo próprio, no prazo estipulado no subitem **11.1**.

11.7. As respostas aos recursos serão disponibilizadas no sistema Comprasnet e no sítio do COFEN.

11.7.1. O licitante, através de consulta permanente aos sítios acima indicados, deverá manter-se atualizado quanto às respostas sobre os recursos interpostos, não cabendo ao COFEN a responsabilidade por desconhecimento de tais informações, em face de inobservância do licitante quanto ao procedimento apontado neste item.

XII. CONTRATAÇÃO DO OBJETO DA LICITAÇÃO

12.1. O representante legal do licitante vencedor deverá comparecer dentro do prazo de 5 (cinco) dias úteis, a contar da data da convocação, para assinatura da Ata de Registro de Preços e do Contrato, conforme o caso, sob pena de decair o direito à contratação.

12.2. A recusa injustificada do licitante vencedor em assinar a Ata de Registro de Preços ou o Contrato, conforme o caso, dentro do prazo e condições estabelecidos, caracterizará o descumprimento total da obrigação assumida, sujeitando-a às penalidades legalmente estabelecidas, além da multa.

12.3. Ocorrendo o previsto em 13.2, o COFEN ou empresa participante do registro convocará observada a ordem de classificação, os demais fornecedores que aceitaram cotar os bens ou serviços com preços iguais aos do licitante vencedor e tiveram seus preços registrados na ata de realização da sessão pública do pregão.

12.3.1. A convocação dos licitantes remanescentes estará condicionada à apresentação dos documentos previstos no item **X** do Edital, conforme § 3º do Art. 11 do Decreto nº 7.892/13.

12.4. Qualquer licitante em vias de ser julgado vencedor, ou já declarado vencedor da licitação, ou já convidado a assinar a Ata de Registro de Preços ou o Contrato, conforme o caso, poderá perder sua condição para fazê-lo se o COFEN vier a ter conhecimento de fato superveniente, comprovado, que o desabone, garantidos o contraditório e a ampla defesa.

XIII. CONDIÇÕES DE PAGAMENTO

13.1. As condições de pagamento estão estabelecidas no Item 8 do Termo de referencia, anexo I deste edital.

XIV. PENALIDADES

14.1. As Sanções Administrativas as quais estão sujeitas a licitante vencedora, estão estabelecidas no Item 10 do Termo de referencia, anexo I deste edital.

XV. DAS OBRIGAÇÕES DA CONTRATADA E DO CONTRANTE

15.1. As obrigações da Contratada e do Contratante as quais estão sujeitas a licitante vencedora e o Cofen, estão estabelecidas nos Itens 4 e 5, do Termo de referencia, anexo I deste edital, respectivamente.

XVI. INFORMAÇÕES, ESCLARECIMENTOS E IMPUGNAÇÕES AO EDITAL.

16.1. Os pedidos de esclarecimentos sobre este procedimento licitatório devem ser enviados ao Pregoeiro, até três (3) dias úteis anteriores à data fixada para abertura da sessão pública, exclusivamente para o endereço eletrônico licitacoes@cofen.gov.br.

16.2. Todo cidadão é parte legítima para impugnar o presente Edital. Qualquer impugnação deverá ser protocolizada até dois (2) dias úteis anteriores à data fixada para abertura da sessão pública, mediante petição a ser enviada exclusivamente para o endereço eletrônico licitacoes@cofen.gov.br.

16.3. Caberá ao Pregoeiro, auxiliado pelo setor responsável pela elaboração do Termo de Referência, decidir sobre a impugnação no prazo de vinte e quatro (24) horas.

16.4. Acolhida a impugnação aos termos deste Edital, designar-se-á nova data para a realização da sessão pública, exceto quando a alteração não afetar a formulação das propostas.
16.5. As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no endereço eletrônico www.comprasnet.gov.br, por meio do seguinte link: acesso livre>pregões>agendados, para conhecimento das licitantes e da sociedade em geral, cabendo aos interessados em participar do certame acessá-lo para obtenção das informações prestadas.

XVII. DAS DISPOSIÇÕES GERAIS

17.1. Para solucionar quaisquer questões oriundas desta licitação, é competente, por disposição legal, o foro da Justiça Federal da sede do Cofen;
17.2. É facultada ao Pregoeiro ou à autoridade superior, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar no ato da sessão pública;
17.3. Fica assegurado ao Cofen o direito de, segundo seu interesse, revogar, a qualquer tempo e motivadamente, no todo ou em parte, a presente licitação, dando ciência aos participantes, na forma da legislação vigente;
17.4. As licitantes assumirão todos os custos de preparação e apresentação de suas propostas e o Cofen não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório;
17.5. O resultado do presente certame será divulgado no D.O.U e no endereço eletrônico www.portalcofen.gov.br;
17.6. Para contagem de prazos neste Edital exclui-se o dia do início e inclui-se o dia do vencimento, considerando-se prorrogado até o 1º dia útil subsequente se o vencimento cair em dia sem expediente no Cofen;

XVIII. FORO

18.1. As partes elegem de comum acordo, a Justiça Federal, no Foro da cidade de Brasília/DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro, por mais privilegiado que seja, para a solução dos conflitos eventualmente decorrentes da presente licitação, nos termos do art. 55, § 2º, da Lei nº. 8.666, de 21 de junho de 1993.

XIX. ANEXOS

19.1. Integram o presente Edital:
a) Anexo I - Termo de Referência;
b) Anexo II – Minuta de Contrato;
c) Anexo III – Modelo de proposta de preços;
d) Anexo IV – Minuta da Ata de registro de preços.

Brasília-DF, _____ de junho de 2017.

Reni Fernandes
Pregoeiro

ANEXO I DO EDITAL

TERMO DE REFERÊNCIA

1. OBJETO

1.1. O presente Termo de Referência tem por objeto a aquisição por meio de **Sistema de Registro de Preços (SRP)**, de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o COFEN, compreendendo o fornecimento, a instalação, o suporte técnico, a garantia, o treinamento, o gerenciamento e o monitoramento de sistemas de: Firewall de Nova Geração (NGFW), Access Point Wireless, Switch PoE, Patch panel, Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web - WAF (Web Application Firewall), Centro de Operações de Segurança da Informação - SOC (Security Operation Center), Teste de Intrusão/Penetração (Pentest), Endpoint, Gestão Contínua de Vulnerabilidades e assinaturas conforme especificações constantes do Anexo I que faz parte deste Termo.

2. JUSTIFICATIVA

2.1. Para atender as demandas preconizadas pelo Planejamento Estratégico do Conselho Federal de Enfermagem - COFEN e Sistema Conselhos Regionais de Enfermagem-COREN, o Departamento de Tecnologia da Informação e Comunicação - DTIC necessita instituir um amplo programa de modernização de suas tecnologias para proteção contra ataques hackers, tentativas de invasão, análise e gestão das vulnerabilidades, integrado às novas tecnologias de segurança da informação, afim de que seja possível o aumento da segurança do ambiente de tecnologia interno e externo ao Órgão. Assim, visa atender aos serviços estratégicos de Tecnologia da Informação e Comunicação do COFEN/COREN por meio da disponibilidade, confidencialidade e integridade das comunicações de dados, imprescindíveis ao bom desempenho e funcionamento das atividades institucionais do COFEN/COREN.

2.2. Cabe ressaltar que, a totalidade dos equipamentos, são destinados a atender ao Conselho Federal de Enfermagem - COFEN e as Unidades dos Conselhos Regionais de Enfermagem que manifestaram interesse em participar da aquisição por meio do SRP. Assim, pretende-se garantir que todos os interessados disponham de infraestrutura de TI adequada e que os usuários tenham acesso aos recursos de processamento com maior disponibilidade, performance, escalabilidade e segurança.

2.3. Registra-se, ademais, que a aquisição será realizada por meio de SRP, conforme inciso II do Art. 3º do Decreto 7.892/2013, uma vez que convém ao COFEN a entrega parcelada dos bens, de acordo com a efetivação das necessidades previstas

3. FUNDAMENTO LEGAL

3.1. A prestação dos serviços objeto deste Termo de Referência obedecerá ao disposto na Lei nº 10.520, de 17/07/2002, Decreto nº. 3.555/2000, Decreto nº 5.450, de 31/05/2005, pela Instrução Normativa SLTI/MP nº 02, de 30 de abril de 2008 e alterações posteriores, Decreto nº 7.892/2013, e subsidiariamente, as normas da Lei nº 8.666/93 e suas alterações.

4. OBRIGAÇÕES DA CONTRATADA

4.1. Além das obrigações decorrentes da aplicação da Lei nº 10.520/02 subsidiariamente da Lei nº 8.666/93, do Decreto nº 5.450/2005, e demais normas pertinentes bem como, as especificações constantes do Anexo I deste Termo de Referência, caberá à Contratada:

4.1.1. Responder, em relação aos seus funcionários, por todas as despesas decorrentes do fornecimento dos produtos e por outras correlatas, tais como salários, seguros de acidentes, tributos,

indenizações, vales-refeição, vales-transporte e outras que porventura venham a ser criadas e exigidas pelo Poder Público;

4.1.2. Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências do Conselho;

4.1.3. Responder pelos danos causados diretamente à Administração ou aos bens do Conselho, ou ainda a terceiros, decorrentes de sua culpa ou dolo, durante a execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Conselho;

4.1.4. Efetuar a troca dos produtos ou manutenção dos serviços que não atenderem às especificações do objeto, no prazo assinado pelo Conselho;

4.1.5. Comunicar ao Conselho qualquer anormalidade constatada e manter, durante o período de vigência do Contrato, o atendimento das condições de habilitação exigidas neste Termo de Referência.

4.1.6. À Contratada caberá assumir a responsabilidade por:

4.1.6.1. Todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com o Conselho;

4.1.6.2. Todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados durante a execução do contrato, ainda que acontecido em dependência do Conselho;

4.1.6.3. Todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução do contrato, originariamente ou vinculada por prevenção, conexão ou continência;

4.1.6.4. Encargos fiscais e comerciais resultantes da contratação resultante deste Termo de Referência.

4.1.7. A inadimplência do licitante vencedor, com referência aos encargos sociais, comerciais e fiscais não transfere a responsabilidade por seu pagamento ao Conselho, nem poderá onerar o objeto desta contratação, razão pela qual o licitante vencedor renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Conselho.

5. OBRIGAÇÕES DO CONTRATANTE

5.1. Além das obrigações decorrentes da aplicação da Lei nº 10.520/02 subsidiariamente da Lei nº 8.666/93 e do Decreto nº 5.450/2005 e demais normas pertinentes bem como, especificações constantes do Anexo I deste Termo, caberá ao Contratante:

5.1.1. Fornecer em tempo hábil, todos os elementos necessários para a prestação dos serviços;

5.1.2. Notificar imediatamente a Contratada sobre qualquer condição operacional anormal;

5.1.3. Efetuar o pagamento devido, segundo as condições estabelecidas;

5.1.4. Oferecer informações à Contratada, sempre que necessárias para execução dos trabalhos;

5.1.5. Aplicar as penalidades previstas no Edital da licitação, na hipótese da Contratada não cumprir com o compromisso assumido, mantidas as situações normais, arcando a empresa com quaisquer prejuízos que tal ato acarretar à Administração.

6. NÍVEIS MÍNIMOS DE SERVIÇO EXIGIDOS (NMSE)

6.1. Para todas as soluções:

6.1.1. Para todas as soluções:

6.1.1.1. A solução deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive sábados, domingos, feriados e no Período de Funcionamento Experimental - PFE;

6.1.1.2. A disponibilidade da solução CONTRATADA corresponde ao percentual de tempo, durante o mês, em que a solução esteve em condições plenas de funcionamento, sem registro de indisponibilidade pelo monitoramento pró-ativo da CONTRATADA e/ou do CONTRATANTE. Tal percentual não poderá ser inferior a 95,0% (noventa e cinco por cento);

6.1.1.3. O percentual mínimo aceitável de disponibilidade mensal de todos os serviços que compõem a solução de segurança de perímetro é de 95,0%. A disponibilidade corresponde ao percentual de tempo, durante um período de 30 dias de operação, em que todos os serviços da solução estiveram em condições normais de funcionamento;

6.1.1.4. Mensalmente, deverá ser calculado o percentual de disponibilidade das soluções, com base na seguinte fórmula:

D = [(43200-Ti)/43200]*100, onde:

- D= Percentual de disponibilidade
- Ti= Somatório dos minutos em que foram observadas inoperâncias em quaisquer dos serviços contemplados pela solução de segurança de perímetro durante o período de faturamento (30 dias);

6.1.1.5. Sempre que forem apurados percentuais de disponibilidade que estejam abaixo do limite mínimo estabelecido (95%), serão aplicadas as penalidades previstas no Edital e seus Anexos.

6.1.2. Para o Serviço de Suporte Técnico:

6.1.2.1. Os serviços de suporte técnico serão prestados vinte quatro (24) horas por dia, sete (7) dias por semana.

6.1.2.2. Os serviços de suporte técnico serão acionados a partir da queda, falha ou registro de indisponibilidade gerado pelo monitoramento (quando for o caso) e/ou por meio de abertura de chamado a critério da equipe técnica do CONTRATANTE. Esses chamados serão classificados conforme as severidades especificadas a seguir:

• Severidade **ALTA**: Esse nível de severidade é aplicado quando há indisponibilidade na solução ou em qualquer serviço que a compõe; para a criação/configuração de políticas nos firewalls; para aplicação de ações de respostas a ataque. Prazo para início do atendimento: 2 horas

• Severidade **MÉDIA**: Esse nível de severidade é aplicado para solicitações de criação/configuração de políticas nos demais serviços que compõem a solução; quando há problema, simultâneo ou não, nos elementos que compõem os serviços/solução, embora ainda estejam disponíveis. Prazo para início do atendimento: 4 horas

• Severidade **BAIXA**: Esse nível de severidade é aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados. Prazo para início do atendimento: 10 horas

6.1.2.3. Faculta-se à CONTRATADA substituir temporariamente o equipamento, peça e componente defeituoso por outros de mesmas características técnicas, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva;

6.1.2.4. O prazo máximo para a substituição temporária será de 30 (trinta) dias, sendo que neste prazo o equipamento, peça e componente substituído deverá ser devolvido à CONTRATANTE em pleno estado de funcionamento ou ser substituído definitivamente;

6.1.2.5. A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer equipamento, peça e componente que venha a se enquadrar em, pelo menos, um dos seguintes casos:

• Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

• Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias.

• No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se à CONTRATADA promover a sua substituição em caráter definitivo;

• A substituição definitiva será admitida com anuência do CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, peça e componente ofertado, em relação àquele que está sendo substituído;

6.1.2.6. A CONTRATADA tornará disponíveis informações sobre desempenho e falhas (indisponibilidade) da solução de forma interativa ("on-line"), a partir do início do Período de Funcionamento Experimental (PFE);

6.1.2.7. Quando da ocorrência de falhas que tornem o serviço/solução indisponível por mais de 30 (trinta) minutos, a CONTRATADA deverá entregar à CONTRATANTE, juntamente com o relatório técnico mensal, a descrição detalhada da ocorrência, suas causas e as ações corretivas realizadas para tornar o serviço/solução novamente disponível;

6.1.2.8. A CONTRATADA deverá manter registro dos eventos, que porventura tenham provocado interrupções na solução dentro do período do faturamento mensal, de modo a justificar à CONTRATANTE a não consideração de tempos de inoperância, causados por falta de energia elétrica nas dependências do CONTRATANTE, por ações ou solicitações do CONTRATANTE ou ainda por manutenções programadas;

6.1.2.9. A CONTRATADA somente poderá efetuar manutenção técnica na solução e seus componentes após aprovação por parte do CONTRATANTE. Caso a manutenção seja efetuada sem essa aprovação, será considerado como indisponibilidade;

6.1.2.10. Será considerado o **Prazo de Solução Definitiva** como o tempo decorrido entre o registro de um chamado e a solução definitiva para efeito dos níveis exigidos.

6.1.2.11. Os chamados de severidade ALTA poderão ser atendidos on-site, a critério do CONTRATANTE. É vedado a CONTRATADA interromper o atendimento até que o serviço seja efetivamente recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. A interrupção do suporte técnico de um chamado desse tipo de severidade por parte da CONTRATADA e que não tenha sido previamente autorizado pelo CONTRATANTE, poderá ensejar em aplicação de penalidades previstas;

6.1.2.12. Após concluído o suporte técnico e com o serviço efetivamente recolocado em pleno estado de funcionamento, a CONTRATADA comunicará o fato à equipe técnica do CONTRATANTE e solicitará autorização para o fechamento do chamado. Caso o CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até o momento em que o serviço seja efetivamente recolocado em pleno estado de funcionamento pela CONTRATADA. Nesse caso, o CONTRATANTE fornecerá por e-mail, telefone ou através da interface de gerenciamento as pendências relativas ao chamado aberto;

6.1.2.13. Caso não haja manifestação dentro do prazo estipulado para o chamado em questão ou caso o CONTRATANTE entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.

6.1.2.14. O CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal de até 10 usuários que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados. Esses perfis serão criados a critério do CONTRATANTE e configurados pela CONTRATADA;

6.1.2.15. Ao detectar tentativas de ataques à rede interna do CONTRATANTE ou aos serviços disponíveis em seu ambiente, a CONTRATADA deverá adotar, de imediato, as medidas de combate ao ataque independentemente das que forem estabelecidas pelo CONTRATANTE. No caso dessas medidas implicarem interrupções e/ou descaracterização dos serviços em uso, a CONTRATADA deverá entrar em contato com o CONTRATANTE em, no máximo, 15 (quinze) minutos, para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las. O CONTRATANTE se responsabilizará por eventuais danos causados pela não autorização de ações recomendadas pela CONTRATADA.

6.1.2.16. Essa lista pode ser ajustada durante o período de vigência do contrato a título de adequação às necessidades do CONTRATANTE mediante anuência e aceite da CONTRATADA, sem ônus para o CONTRATANTE.

6.1.3. Pelo não cumprimento do índice mínimo de DISPONIBILIDADE previsto, serão aplicadas as penalidades previstas em Contrato.

7. FISCALIZAÇÃO

7.1. A fiscalização da execução do objeto do contrato será exercida por servidor nomeado pelo Contratante, nos termos do artigo 67 e 73 da Lei nº 8.666/93;

7.2. Ao Contratante reserva-se o direito de rejeitar, no todo ou em parte, os itens/serviços fornecidos em desacordo com o estabelecido no presente Termo de Referencia;

7.3. A fiscalização exercida pelo Gestor do Contratante não excluirá ou reduzirá a responsabilidade da Contratada pela completa e perfeita execução dos itens deste Termo de Referência e seus anexos.

8. FORMA E CONDIÇÕES DE PAGAMENTO

8.1. O pagamento será realizado sob demanda executada, no mês subsequente a realização do serviço, de acordo com a quantidade atendida, após o cumprimento das etapas de implantação e efetiva utilização dos serviços, desde que todos os serviços estejam atestados pelo gestor;

8.2. O Cofen efetuará o pagamento, em moeda nacional corrente, por meio de Ordem Bancária, no prazo de 10 (dez) dias úteis, contados a partir da emissão do termo de aceite pelo gestor do contrato, juntamente com a entrega da Nota Fiscal/Fatura;

8.3. Ocorrendo a não aceitação pela fiscalização do Cofen dos serviços faturados, o fato será imediatamente comunicado à Contratada, para retificação das causas de seu indeferimento;

8.4. A nota fiscal deve estar preenchida com a descrição detalhada dos itens do objeto, o número do Contrato e os dados bancários da Contratada;

8.4.1. Junto com a Nota Fiscal, deverá apresentar a comprovação de regularidade, junto ao Sistema da Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (FGTS), às Fazendas Federal, Estadual e Municipal do domicílio ou sede da Contratada e da certidão negativa de débitos trabalhistas (CNDT), sem que isso gere direito a alteração de preços ou compensação financeira.

8.4.2. O não envio das certidões juntamente com as notas fiscais, ou ainda que as mesmas estejam disponíveis para emissão, não desobriga o Cofen de efetuar o pagamento das Notas Fiscais que constem serviços devidamente prestados e atestados pelo gestor do Contrato. Porém o desatendimento pela Contratada ao descrito pode motivar a rescisão contratual, a execução da garantia para ressarcimento dos valores e indenizações devidas à Administração e a aplicação das penalidades previstas no art. 87 da Lei nº 8.666/93.

8.5. Os pagamentos poderão ser descontinuados pelo Cofen, nos seguintes casos:

a) Não cumprimento das obrigações da Contratada para com terceiros, que possam, de qualquer forma, prejudicar o Cofen;

b) Inadimplemento de obrigações da Contratada para com o Cofen por conta do Contrato;

c) Erros ou vícios nas faturas.

8.6. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes formulas:

$$I = \frac{(TX/100)}{365}$$

EM = I x N x VP, onde:
I = Índice de atualização financeira;
TX = Percentual da taxa de juros de mora anual;
EM = Encargos moratórios;
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = Valor da parcela em atraso.

8.7. Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos, e ser submetidos à apreciação da autoridade superior competente, que adotará as providências para verificar se é ou não caso de apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa;
8.8. Não será efetuado nenhum pagamento antecipado, nem por serviços não executados.

9. PRAZO DE VIGÊNCIA DO CONTRATO

9.1. O prazo de vigência do contrato será no máximo de 12 (doze) meses, contados a partir da assinatura do contrato, com eficácia após a publicação de seu extrato no Diário Oficial da União. O prazo previsto poderá ser prorrogado na ocorrência quaisquer das hipóteses descritas nos incisos I a IV do parágrafo primeiro do artigo 57 da Lei 8.666/93, desde que seja apresentada justificativa por escrito até o 10º (décimo) dia útil anterior ao termo final do prazo pactuado.

10. SANÇÕES ADMINISTRATIVAS

10.1. Com fundamento no artigo 7º da Lei n.º 10.520/2002 e no art. 28 do Decreto n.º 5.450/2005, ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e será descredenciada do Sicaf e do cadastro de fornecedores da Contratante, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo das demais cominações legais e de multa de até 30% (trinta por cento) sobre o valor da contratação, sem prejuízo da rescisão unilateral do contrato (art. 78 da Lei 8.666, de 1993), a Contratada que:

10.1.1. não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;

10.1.2. apresentar documentação falsa;

10.1.3. deixar de entregar os documentos exigidos no certame;

10.1.4. ensejar o retardamento da execução do objeto;

10.1.5. não mantiver a proposta;

10.1.6. cometer fraude fiscal;

10.1.7. comportar-se de modo inidôneo;

10.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.

10.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

10.3.1. Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

10.3.2. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

10.4. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

10.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

10.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

11. ALTERAÇÃO SUBJETIVA

11.1. É admissível a fusão, cisão ou incorporação da Contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa do Contratante à continuidade do contrato.

12. GARANTIA CONTRATUAL

12.1. A Contratada deverá apresentar no prazo máximo de 10 (dez) dias, contados da data de assinatura do instrumento contratual, garantia de **5%** (cinco por cento) do valor contratual estimado para 12 (doze) meses, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, nos termos do Paragrafo 1º do artigo 56, da Lei nº 8.666/93;

12.2. A garantia assegurará qualquer que seja a modalidade escolhida, o pagamento de:

12.2.1 Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

12.2.2 Prejuízos causados ao Contratante ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

12.2.3 As multas moratórias e punitivas aplicadas pelo Contratante à Contratada;

12.2.4 Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela contratada;

12.3. A contratada se obriga a apresentar a garantia para o período integral da vigência contratual, e, no caso de prorrogação do contrato, mantê-la válida e atualizada;

12.4. A perda da garantia em favor do Contratante, por inadimplemento das obrigações contratuais, far-se-á de pleno direito, independente de qualquer procedimento judicial ou extrajudicial das demais sanções previstas no contrato;

12.5. A garantia deverá ser integralizada sempre que dela forem deduzidos quaisquer valores e nos casos de prorrogação de prazo ou acréscimo de valores deverá ser atualizada na mesma proporção em conformidade com o art. 56, § 2º da Lei 8.666/93;

12.6. A qualquer tempo poderá ser admitida a substituição da garantia, observadas as modalidades previstas no artigo 56 da Lei nº 8.666/93;

12.7. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento);

12.8. O atraso superior a 30 (trinta) dias autoriza o Contratante a promover a retenção dos pagamentos devidos à Contratada, até o limite de 5% (cinco por cento) do valor anual do contrato, a título de garantia, com correção monetária, em favor da contratada;
12.9. Será considerada extinta a garantia:

12.9.1 Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

12.9.2 Com a extinção do contrato.

12.10. A garantia sempre terá prazo de cobertura findando 03 (três) meses, após, o término da vigência contratual, conforme inciso XIX do art. 19 da Instrução Normativa nº 06, de 23 de dezembro de 2013.
12.11. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Contratante, com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

13. RECURSOS ORÇAMENTARIOS

13.1. Os recursos orçamentários necessários ao atendimento do objeto deste Termo de Referencia correrão pelo Orçamento do Cofen no exercício de 2015 e 2016, e serão alocados pelo Departamento Financeiro deste Conselho.

14. DISPOSIÇÕES GERAIS

14.1. O valor final para o cumprimento do objeto do presente Termo de Referência será definido após a Cotação Prévia de Preços, que será realizada pelo Setor de Compras e Contratações.
14.2. O Contratante poderá realizar acréscimos ou supressões nas quantidades inicialmente previstas, respeitados os limites do artigo 65 da Lei 8.666/93 e suas alterações, tendo como base os preços constantes da proposta da Contratada.
14.3. O Contratante se reserva o direito de paralisar ou suspender, a qualquer tempo, a execução dos serviços, mediante pagamento único e exclusivo dos trabalhos já executados, por ajuste entre as partes interessadas, dos materiais existentes no local dos serviços, e a ele destinados.

Elaborado pela ASTEC.

ANEXO I
Especificação Técnica

PROJETO ATIVIDADE: Ampliação e Aprimoramento da Tecnologia da Informação

FUNDAMENTAÇÃO MÍNIMA PARA AQUISIÇÃO DOS BENS E SERVIÇOS

1. OBJETO SINTÉTICO

1.1. Aquisição de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o COFEN, compreendendo o fornecimento, a instalação, o suporte técnico, a garantia, o treinamento, o gerenciamento e o monitoramento de sistemas de: Firewall de Nova Geração (NGFW), Access Point Wireless, Switch PoE, Patch panel, Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web - WAF (Web Application Firewall), Centro de Operações de Segurança da Informação - SOC (Security Operation Center), Teste de Intrusão/Penetração (Pentest), Endpoint, Gestão Contínua de Vulnerabilidades e assinaturas conforme especificações constantes dos Anexos que fazem parte deste Edital.

2. OBJETIVO GERAL

2.1. O certame visa municiar a CONTRATADA com Soluções de Segurança da Informação, Infraestrutura de rede e mão de obra especializada.

3. OBJETIVO ESPECÍFICO

3.1. Prover o COFEN com as seguintes soluções:

- **3.1.1.** Sistema de Firewall de Nova Geração (NGFW)
- **3.1.2.** Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall)
- **3.1.3.** Sistema de Segurança para Endpoint
- **3.1.4.** Solução de Comunicação para Redes Wireless
- **3.1.5.** Sistema de Gestão Contínua de Vulnerabilidades
- **3.1.6.** Suporte da Solução
- **3.1.7.** Centro de Operações de Segurança da Informação - SOC (Security Operation Center)
- **3.1.8.** Implantação da Solução
- **3.1.9.** Treinamento da Solução
- **3.1.10.** Workshop de Atualização
- **3.1.11.** Teste de Intrusão/Penetração (Pentest)

4. QUANTIFICAÇÃO DOS SERVIÇOS - LOTES E ITENS

Lote	Descrição	Qtde	Forma de Desembolso
1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A	1	Único
	Implantação da Solução	1	
	Treinamento da Solução	1	
	WorkShop de atualização	4	
	Suporte da Solução – Item 11.4	1	
2	Sistema de Firewall de Nova Geração (NGFW) –	1	Único

	TIPO B		
	Implantação da Solução	1	
	Treinamento da Solução	1	
	WorkShop de atualização	4	
	Suporte da Solução – Item 11.4	1	
3	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance FÍSICO	1	Único
	Implantação da Solução	1	
	Treinamento da Solução	1	
	WorkShop de atualização	4	
	Suporte da Solução – Item 11.4	1	
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	1	Único
	Implantação da Solução	1	
	Treinamento da Solução	1	
	WorkShop de atualização	4	
	Suporte da Solução – Item 11.4	1	
5	Sistema de Segurança para Endpoint – 50 licenças	1	Único
	Implantação da Solução	1	
	Treinamento da Solução	1	
	WorkShop de atualização	4	
	Suporte da Solução – Item 11.4	1	
6	Solução de Comunicação para Redes Wireless - AP	1	Único
	Implantação da Solução	1	
	Treinamento da Solução	1	
	Suporte da Solução – Item 11.4	1	
7	Solução de Comunicação para Redes Wireless – Switch PoE	1	Único
	Implantação da Solução	1	
	Treinamento da Solução	1	
	Suporte da Solução – Item 11.4	1	
8	Solução de Comunicação para Redes Wireless – Patch Panel	1	Único
	Instalação	1	
9	Sistema de Gestão Contínua de Vulnerabilidades	1	Único
	Implantação da Solução	1	
	Treinamento da Solução	1	
	WorkShop de atualização	4	
	Suporte da Solução – Item 11.4	1	
10	Centro de Operações de Segurança – SOC (Security Operation Center)	1	Mensal
11	Serviço de Teste de Intrusão/Penetração (Pentest)	2	Semestral

4.1. Devido ao possível conflito de interesses entre os prestadores de serviços no Lote 11 com os demais (exceção ao Lote 8), uma mesma empresa participante não poderá prestar os serviços do Lote 11 concomitantemente com outro Lote (exceção ao Lote 8), ou seja, se uma mesma empresa

vencer a concorrência deste Lote – juntamente com outro(s) Lote(s), deverá optar pelo tipo de serviço que deseja fornecer.

5. JUSTIFICATIVA

5.1. Para atender as demandas preconizadas pelo Planejamento Estratégico do Conselho Federal de Enfermagem – COFEN, o Departamento de Tecnologia da Informação e Comunicação – DTIC necessita instituir um amplo programa de modernização de suas tecnologias para proteção contra ataques hackers, tentativas de invasão, análise e gestão das vulnerabilidades, integrado às novas tecnologias de segurança da informação, afim de que seja possível o aumento da segurança do ambiente de tecnologia interno e externo ao Órgão. Assim, visa atender aos serviços estratégicos de TIC do COFEN por meio da disponibilidade, confidencialidade e integridade das comunicações de dados, imprescindíveis ao bom desempenho e funcionamento das atividades institucionais do COFEN.

6. MOTIVAÇÃO DA CONTRATAÇÃO

6.1. O DTIC gerencia os serviços de Internet e utiliza uma solução de Firewall que viabiliza a filtragem dos conteúdos que são acessados internamente e promove a proteção da rede interna do Conselho contra acessos externos indevidos.
6.2. O serviço não prevê, entretanto, proteção contra ataques ou explorações de vulnerabilidades provenientes e destinadas às redes internas, ou seja, todos os canais de comunicação das unidades do COFEN têm acesso liberado entre si. Dessa forma, máquinas infectadas por códigos maliciosos em uma determinada unidade podem ser a causa de problemas em outras unidades, já que a ausência de inspeção do tráfego interno propicia este tipo de ocorrência.
6.3. O bom uso dos recursos de tecnologia da informação, principalmente no que tange a qualidade da navegação web das unidades do COFEN, é um dos principais fatores que nortearam a elaboração do presente projeto, pois os usuários possuem seus perfis identificados e tratados localmente, com liberações e restrições de acesso que os acompanham pelas estações de trabalho que estiverem utilizando. Uma política de liberação de acesso web mais adequado às necessidades institucionais que respeite as especificidades de cada unidade, precisa se fazer presente.
6.4. O COFEN vem ao longo dos últimos anos realizando investimentos significativos na informatização de suas atividades, fato que permitiu o tratamento do crescente volume de dados, gerado em decorrência do aumento considerável de tráfego em sua rede lógica, acrescido de variado conjunto de informações utilizado para as mais diversas finalidades. No entanto, para que tais informações funcionem efetivamente como ferramenta de trabalho para os usuários do COFEN é preciso assegurar que tais informações estarão disponíveis no momento em que forem necessárias e que tenham sua integridade e atualizações asseguradas com acompanhamento eficiente por parte dos administradores da rede.
6.5. Adicionalmente, deverá ser observado que o conjunto de informações hoje existente no âmbito do COFEN constitui um importante patrimônio público, tornando-se, portanto imprescindível a adoção de medidas para sua manutenção e preservação.
6.6. A vista do exposto, é escopo do presente termo de referência delinear os requisitos dos serviços de segurança da informação a serem contratados, bem como especificá-los para garantir um perfeito funcionamento da rede e satisfação dos seus usuários.
6.7. Trata-se de uma iniciativa que busca a otimização dos processos administrativos e maior eficiência operacional da gestão da Infraestrutura de Segurança do COFEN, observando que o projeto busca gerar condições de fornecimento de soluções numa perspectiva de serviço de maneira que as demandas sejam atendidas de maneira mais rápida e assertiva, suportando operações que impliquem em um ambiente seguro e confiável tanto para os colaboradores do COFEN quanto para o público externo.

6.8. A contratação do serviço possibilitará qualificar a administração de TI, tornando-a efetivamente comprometida com a qualidade dos serviços, com excelência de gestão e, principalmente com as áreas de negócios do COFEN.
6.9. O COFEN encontra-se num momento de crescimento e expansão, sua rede tem sido cada vez mais acessada, tornando-se imperativo que o ambiente tecnológico interno esteja disposto de forma estável, robusta e confiável, os sistemas atualmente em uso não cobrem todas as camadas de rede do tráfego existente. Esta forma de utilização não protege o ambiente contra as vulnerabilidades existentes atualmente, o que fatalmente resultará em indisponibilidade do ambiente. Camadas de proteção avançada poderiam dotar o COFEN de uma infraestrutura de segurança mais robusta e confiável.
6.10. A crescente dependência da tecnologia da informação em diversas áreas da organização torna imprescindível esse projeto com foco na segurança da informação, principalmente em face da expansão dos Sistemas Corporativos desenvolvidos e internalizados pelo Departamento de Tecnologia da Informação utilizado pelos Regionais, Profissionais e a sociedade em geral.
6.11. Há no COFEN um histórico de ataques e infestação de vírus, que comprometeram a disponibilidade dos serviços da instituição e um relatório de auditoria realizado antes das Eleições via Internet que apresentou algumas vulnerabilidades nos sistemas Web do COFEN que precisavam ser sanadas.
6.12. A principal vantagem da contratação de serviços estará na atividade de monitoramento permanente, apta a propiciar pronta resposta a eventuais incidentes ocorridos na operação diária. Esta infraestrutura estará ligada diretamente à gestão do ambiente tecnológico do COFEN, e será dotada de infraestrutura física, ferramentas integradas de inteligência e de comunicação, assim como sistemas tecnológicos complexos, capazes de prover informações necessárias à tomada de decisão, à emissão de ordens e ao acompanhamento de ações, que procuram como resultado final prover um ambiente mais confiável e estável aos usuários internos e externos.
6.13. Além de aumentar a segurança de toda a rede local do COFEN, o serviço prevê solução de filtragem e proteção de intrusão, camada adicional contra-ataques de aplicação e serviços de resposta a incidente de segurança. O conjunto do projeto permitirá a implementação de políticas de segurança globais e/ou diferenciadas para os usuários, além de facilitar a administração dos incidentes de segurança.

7. SOLUCOES REQUERIDAS E RESULTADOS ESPERADOS

7.1. A Segurança da Informação é um processo e a segurança de estações, servidores, usuários e das informações corporativas não basta ser composta apenas de antivírus e um firewall de bloqueio de portas.
7.2. As ameaças, que podem ser internas ou externas, vêm aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas com múltiplas camadas de proteção, de forma a reduzir o risco, minimizando a probabilidade e os impactos de um eventual ataque cibernético.
7.3. O fluxo constante de complexas e evoluídas ameaças como worms, spywares, cavalos de Tróia, hackers, ladrões de identidade e diversos outros tipos de ataques ameaçam os dispositivos conectados à Internet.
7.4. Os danos causados pelas pragas virtuais podem comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações, serviços e operações de rede, atingindo recursos essenciais para o bom funcionamento dos ativos da instituição, o que inclui seus bens tangíveis e intangíveis, como a reputação da instituição perante a sociedade.
7.5. Dessa forma, objetivando minimizar os riscos, o COFEN necessita implantar uma solução corporativa de gerenciamento da segurança. A implantação da solução deverá permitir a identificação das tentativas de invasão aos sistemas do COFEN, identificar e mitigar as vulnerabilidades existentes, protegendo a Instituição de uma grande gama de ataques internos e

externos e visará aderência aos objetivos estratégicos e metas da "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018, versão 1.0" cujas diretrizes aplicam-se a todos os órgãos e entidades que integram a APF.

7.6. Baseado nas motivações e fundamentações expostas apresenta-se ações que visam resolver os problemas enfrentados:

7.6.1. Implantação de uma solução que atue proativamente contra códigos maliciosos de qualquer natureza com atualizações constantes;

7.6.2. Implantação de uma solução que analise, controle e que faça o balanceamento dos diferentes tipos de tráfego atualmente utilizados na Internet e que também compreenda os novos paradigmas de segurança baseado em comportamento, reputação e tráfego criptografado.

7.6.3. Implantação de uma solução que gerencie os equipamentos diversificados que ingressam na rede corporativa do COFEN, pelos diversos meios, incluindo via sem fio, e que garanta que suas atividades sejam compatíveis com a finalidade do uso dos serviços disponibilizados pelo COFEN e que não comprometa o bom desempenho da Rede e a segurança, mitigando potenciais vulnerabilidades.

7.6.4. Implantação de uma solução que controle o tráfego da rede sem fio corporativa e a disponibilidade, integridade, confidencialidade e autenticidade dos dados trafegados.

7.6.5. Implantação de uma solução que controle e filtre os acessos a conteúdos e programas (softwares) nos diversos computadores e notebooks da instituição, garantindo que somente os programas e conteúdos destinados aos fins de pesquisa e desenvolvimento de trabalhos do COFEN sejam acessados.

7.6.6. Implantação de uma solução que proteja os sistemas hospedados na infraestrutura interna do COFEN, e por vezes disponibilizados pela Internet para outras instituições públicas e privadas e também para sociedade.

7.6.7. Implantação de uma solução que permita a comunicação segura entre o COFEN os Conselhos Regionais assim como os funcionários e colaboradores que realizam atividades remotamente.

7.6.8. Implantação de uma solução que monitore os diferentes serviços disponibilizados pelo COFEN e que são suportados em diversas plataformas tecnológicas de forma a possibilitar a atuação proativa do Departamento de TIC do COFEN na manutenção da disponibilidade dos serviços.

7.6.9. Implantação de uma solução que investigue minuciosamente a rede corporativa do COFEN, tanto na infraestrutura quanto nos sistemas e ferramentas de apoio, em busca de potenciais vulnerabilidades nos diversos serviços e estruturas, dentro e fora do COFEN e que auxilie na extinção ou minimização dos riscos de eventuais vulnerabilidades.

7.6.10. Esta Solução de Segurança deve permitir uma visualização global dos níveis de segurança em que se encontra a rede de comunicações de dados do COFEN e a tomada de ações imediatas para adequá-la ao nível de segurança aceitável.

8. CONTINUIDADE DO NEGÓCIO

8.1. A aquisição dos bens irá aumentar a proteção do ambiente computacional do COFEN pelo período de até 60 (sessenta) meses. A mera aquisição dos equipamentos que integram a solução não seria suficiente para a plena implementação da segurança, visto que equipamentos de segurança geram registros que devem ser monitorados vinte e quatro (24) horas do dia, sete (7) dias por semana, demanda difícil de ser atendida no serviço público devido a políticas de jornada de trabalho, sobreaviso e de pessoal. Essa demanda de 24x7 ocorre devido à necessidade da disponibilização de diversos sistemas que operam via Internet para os regionais em fusos horários diversos que acessam informações e sistemas do COFEN, para as atividades laborais de empregados do COFEN que requerem a disponibilidade dos sistemas e serviços em horários especiais e ainda da necessidade dos serviços de manutenção que operam no período noturno.

8.2. Além da aquisição dos bens, há a questão do serviço de subscrição, uma assinatura de bases de dados de atualização que contém informações de pragas virtuais, de reputação de endereços da Internet, de padrões de comportamento próprios e impróprios e outros. Sem esse serviço de subscrição, as atualizações necessárias à utilização dos módulos deixariam de ser obtidas, tornando praticamente inócua uma importante parte da solução com relação à capacidade do dispositivo quanto à qualidade e à eficiência técnica, a constante evolução das ameaças e a correspondente necessidade de resposta dos algoritmos de detecção e prevenção de intrusão e códigos maliciosos que formam desafios difíceis de serem continuamente superados exigindo assim atualizações constantes dos módulos responsáveis pelas contramedidas.
8.3. Diante do exposto, a título de continuidade do negócio é solicitado o fornecimento de garantia de atualização e de subscrição de assinaturas e bases de dados para os produtos integrantes da solução por até 60 (sessenta) meses.

9. RESULTADOS ESPERADOS

9.1. As expectativas que se tem do ponto de vista de resultados:

9.1.1. Operações contábeis mais seguras;

9.1.2. Prestação de contas junto ao COFEN facilitada, através de um ambiente tecnológico mais confiável;

9.1.3. Menor tempo de indisponibilidade do ambiente e dos serviços;

9.1.4. Maior qualificação da mão de obra na execução;

9.1.5. Fornecimento de serviços de tecnologia mais estáveis;

9.1.6. Parque tecnológico das unidades gestoras seguro contra ataques ou invasões;

9.1.7. Capacidade de planejamento, de priorização e alocação de recursos melhorados;

9.1.8. Desempenho institucional e profissional incrementado;

9.1.9. Conhecimentos adquiridos multiplicados;

9.1.10. Uso de práticas inovadoras e bem-sucedidas.

10. PRAZO PARA EXECUÇÃO DOS SERVIÇOS

10.1. A CONTRATADA deverá instalar a solução na Sede do CONTRATANTE em até 60 (sessenta) dias após a assinatura do contrato. Na reunião de Alinhamento de Expectativas, deverá ser apresentado o Plano de Implantação pela CONTRATADA conforme item **11.6**, para análise e aprovação do CONTRATANTE.
10.2. Os serviços serão executados conforme matriz de implantação do projeto a ser definida pela equipe técnica do COFEN, considerando o tempo gasto para a preparação da infraestrutura básica de funcionamento, migração de dados, implantação, capacitação, treinamento e de adequações necessárias ao início do funcionamento do sistema.

11. DETALHAMENTO DOS ITENS DO OBJETO

11.1. Documentação Técnica e Acessórios

11.1.1. Deverá ser entregue pela CONTRATADA a "Documentação Técnica" (DT) de toda a solução implementada no ambiente do CONTRATANTE, inclusive com as configurações específicas e topologias. Essa documentação fica sujeita à análise e à aprovação da equipe técnica do CONTRATANTE;

11.1.1.1. Toda a DT deverá ser entregue em uma via impressa e uma via em mídia digital, devendo as topologias e os diagramas lógicos da solução serem entregues em formato “vsd” compatível com o padrão utilizado pelo CONTRATANTE;

11.1.1.2. A DT deverá conter também um conjunto de procedimentos necessários para abertura de chamados de Suporte Técnico; para emissão de relatórios das ferramentas utilizadas na solução, entre outros.

11.2. Garantia

11.2.1. A garantia deve compreender a correção de falhas nos produtos, independentemente de correções tornadas públicas, desde que tenham sido detectadas e formalmente comunicadas à CONTRATADA.

11.2.2. Caso sejam detectadas falhas ou *bugs* nos produtos, a empresa CONTRATADA deverá realizar as atualizações necessárias à correção do problema.

11.2.3. Os produtos devem ser isentos de malwares, inclusive backdoors.

11.2.4. Todos os produtos fornecidos deverão possuir garantia de funcionamento durante a vigência do Contrato.

11.2.5. A CONTRATADA deverá garantir a atualização dos microcódigos, firmwares, drivers e softwares instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato.

11.2.6. A CONTRATADA é a única responsável pelos produtos fornecidos à CONTRATANTE, mesmo que tenham sido adquiridos de terceiros.

11.2.7. A garantia de cada produto deve iniciar-se após a emissão do Termo de Recebimento Definitivo.

11.2.8. O Termo de Recebimento Definitivo será emitido em até três (3) dias úteis após a conclusão do PFE - Período de Funcionamento experimental.

11.2.9. A CONTRATADA responderá pela reparação dos danos causados por defeitos relativos ao serviço prestado. Por isso deverá prezar pela qualidade e eficiência, garantindo que o serviço e também as soluções definitivas fornecidas não causem problemas adicionais àqueles apresentados pelo CONTRATANTE quando da abertura dos chamados de suporte técnico.

11.2.10. Caberá à CONTRATADA apresentar novas soluções dentro dos prazos e condições estabelecidas nos Acordos de Níveis de Serviço (ANS), sem prejuízo de aplicação de penalidades previstas, caso sejam detectados erros ou impropriedades na solução apresentada.

11.2.11. Todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de *end-of-sale*, *end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia pelo período da contratação.

11.2.12. A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do contrato, totalizando 60 (sessenta) meses, nas capitais dos Estados e no Distrito Federal, a contar da data do recebimento definitivo da solução.

11.2.13. A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas por 60 (sessenta) meses, nas capitais dos Estados e no Distrito Federal, sem ônus adicional para o CONTRATANTE.

11.3. Atualizações e Assinaturas

11.3.1. No que se refere a software, durante a vigência do Contrato, a CONTRATADA deverá prover toda e qualquer atualização dos produtos, incluindo vacinas, assinaturas, bases de dados, novas versões lançadas ou novos produtos que venham a substituí-lo no mercado, sem ônus adicional para o CONTRATANTE;

11.3.2. Para fins desta especificação técnica, entende-se como atualização o provimento de toda e qualquer evolução do produto, incluindo:

11.3.2.1. Patches, fixes, correções, updates e service packs;

11.3.2.2. Novas releases, builds e funcionalidades;

11.3.2.3. O provimento de upgrades para novas versões de mercado ou lançamentos, independente da simples alteração cosmética do nome do produto ou do fato do produto ter sido reescrito;

11.3.2.4. O provimento de upgrades englobando, inclusive, versões não sucessivas, caso a disponibilização de tais versões ocorra durante o período da vigência do Contrato;

11.3.2.5. No caso de descontinuidade do produto, o mesmo deverá ser substituído pelo seu sucedâneo.

11.3.2.6. A cada nova liberação de versão e release, a CONTRATADA deverá apresentar as atualizações, inclusive de manuais e demais documentos técnicos, bem como nota informativa das novas funcionalidades implementadas, se porventura existirem.

11.3.3. A CONTRATADA deverá fornecer tais atualizações independentemente de solicitação expressa do CONTRATANTE;

11.3.4. A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução, que deverão permanecer ativas e válidas pelo prazo de validade do contrato;

11.3.5. As licenças de uso de software necessárias para o funcionamento dos equipamentos de segurança serão adquiridas em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante ou seu representante.

11.3.6. Toda intervenção técnica deve ser realizada com anuência do CONTRATANTE.

11.4. Suporte técnico

11.4.1. O Suporte Técnico deve iniciar-se após a emissão do Termo de Recebimento Definitivo estendendo-se por todo o período de vigência do Contrato;

11.4.2. O Suporte Técnico deverá cobrir a localidade da CONTRATADA.

11.4.3. Serviços de manutenção de hardware “on-site”, nas dependências da CONTRATANTE, obrigatoriamente executados por Assistência Técnica e Suporte autorizados pelo Fabricante credenciada através de declaração do Fabricante e com técnicos treinados e certificados nos equipamentos ofertados ou diretamente pelo Fabricante dos produtos.

11.4.4. O Suporte Técnico de todos os produtos deverá abranger a assistência técnica preventiva e corretiva com a cobertura de todo e qualquer defeito apresentado, inclusive, e não se restringindo a: substituição total ou parcial do produto como peças, partes, componentes e acessórios;

11.4.5. A assistência técnica preventiva é todo procedimento planejado cuja ação implementada, seja qual for, visa evitar que o(s) produto(s) fornecido(s) venha(m) a ficar inoperante(s) ou apresentar baixo desempenho;

11.4.6. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

11.4.7. Deverão ser abertos chamados de severidade Alta ou Média para a realização da assistência técnica corretiva;

11.4.8. Os serviços de assistência técnica preventiva e/ou corretiva serão prestados a todos os produtos fornecidos pela CONTRATADA. A prestação desses serviços deve ser realizada nas dependências do CONTRATANTE, onde se encontrarem instalados esses produtos, ou remotamente quando autorizado pelo CONTRATANTE. Esses serviços de assistência técnica deverão ser executados pela CONTRATADA sempre que se fizer necessário, através da solicitação por parte do CONTRATANTE;

11.4.9. O CONTRATANTE poderá, a qualquer momento, determinar à CONTRATADA a execução das rotinas de assistência técnica preventiva e/ou corretiva nos produtos fornecidos;

11.4.10. A CONTRATADA deverá executar a assistência técnica preventiva e/ou corretiva nos produtos fornecidos sempre que solicitado;

11.4.11. A realização de assistência técnica preventiva, caso não seja solicitada pelo CONTRATANTE, deverá ser comunicada à mesma com antecedência mínima de dois (2) dias úteis, devendo o horário ser negociado de forma a não haver impacto no ambiente de produção do CONTRATANTE;

11.4.12. Todas as despesas decorrentes da necessidade de substituição dos produtos, transporte, deslocamento, embalagem, peças, partes, manuais do fabricante, serão de inteira responsabilidade da CONTRATADA, não devendo gerar qualquer ônus adicional à CONTRATANTE;

11.4.13. A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do CONTRATANTE, caso requeiram;

11.4.14. A CONTRATADA será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante toda a vigência do Contrato;

11.4.15. Durante o período de garantia, a CONTRATADA compromete-se a substituir, em até 10 (dez) dias úteis, sem qualquer ônus para o CONTRATANTE, os equipamentos que apresentarem, em um período de 30 (trinta dias), duas ocorrências de defeitos por inoperância de produto ou 3 (três) ocorrências de deficiência operacional do produto, de acordo com o item 11.5.2.5. Neste caso, as novas unidades empregadas na substituição das defeituosas ou danificadas deverão ter prazo de garantia igual ou superior ao das substituídas;

11.4.16. A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço de atendimento com discagem gratuita (0800 ou de custo local DDD) ou qualquer outro meio de comunicação de disponibilidade imediata (por exemplo, sítio Web com HTTPS ou call center), sem ônus adicional para o CONTRATANTE, para chamada do serviço de suporte técnico que deverá estar acessível durante 24h x 7; horário local de Brasília.

11.4.17. O suporte aos componentes do serviço deve compreender o acesso a helpdesk para abertura/acompanhamento de chamados em língua portuguesa, incluindo o atendimento telefônico e o atendimento via e-mail ou sítio Web;

11.4.18. Os serviços de atendimento e de suporte deverão, no acionamento, registrar o chamado, protocolar a data e hora da solicitação, nome do SOLICITANTE, descrição detalhada da solicitação;

11.4.19. O serviço de suporte deverá ser efetuado on-site sempre que se fizer necessário ou quando for solicitado pelo CONTRATANTE;

11.4.20. Deverá cobrir todo e qualquer defeito apresentado na solução, incluindo esclarecimentos técnicos para ajustes, reparos, instalações, configurações e correções necessárias;

11.4.21. Se durante as manutenções for verificada a necessidade de substituição de peça e/ou componente dos equipamentos, essa deverá ocorrer sem custo adicional para o CONTRATANTE;

11.4.22. No caso de substituição temporária, o equipamento, peça e componente deverá possuir, no mínimo, características técnicas e desempenho iguais ou superiores às substituídas com a anuência do CONTRATANTE. Deverão ainda ser homologadas pelo fabricante dos equipamentos;

11.4.23. No caso de substituição definitiva, o equipamento, peça e componente deverá possuir, no mínimo, características técnicas e desempenho iguais ou superiores às substituídas, serem novas, de primeiro uso e homologadas pelo fabricante dos equipamentos e deve pertencer à linha de produção atual do fabricante;

11.4.24. Caso seja necessário enviar o equipamento, peça e componente para um centro de assistência técnica fora das dependências do CONTRATANTE, a CONTRATADA deverá desinstalar, embalar, transportar e reinstalar, bem como deverá arcar com todos os custos necessários;

11.4.25. O envio de equipamentos para centros de assistência técnica em outra localidade a CONTRATADA poderá renegociar os prazos estabelecidos nos níveis de serviço exigidos;

11.4.26. Para a remoção de equipamento, peça e componente será necessária autorização de saída por escrito emitida por servidor do CONTRATANTE, a ser concedida ao funcionário da CONTRATADA, formalmente identificado;

11.4.27. Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá imediatamente abrir um chamado técnico, informar à CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos nos acordos de níveis de serviço;

11.4.28. A CONTRATADA encaminhará mensagem de e-mail para o CONTRATANTE em endereço a ser disponibilizado para esse fim informando o número de cada chamado técnico aberto e sua descrição, independente da forma, seja pelo monitoramento proativo da CONTRATADA e/ou por meio de abertura de chamado a critério da equipe técnica do CONTRATANTE conforme severidades e necessidades especificadas, que servirá de referência para acompanhamento dos atendimentos.

11.5. Acordo de Nível de Serviço (ANS) e Disponibilidade - válidos para todos os produtos/serviços fornecidos pela CONTRATADA;

11.5.1. Para todas as soluções:

11.5.1.1. A solução deverá estar disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, inclusive sábados, domingos, feriados e no Período de Funcionamento Experimental - PFE;

11.5.1.2. A disponibilidade da solução CONTRATADA corresponde ao percentual de tempo, durante o mês, em que a solução esteve em condições plenas de funcionamento, sem registro de indisponibilidade pelo monitoramento pró-ativo da CONTRATADA e/ou do CONTRATANTE. Tal percentual não poderá ser inferior a 95,0% (noventa e cinco por cento);

11.5.1.3. O percentual mínimo aceitável de disponibilidade mensal de todos os serviços que compõem a solução de segurança de perímetro é de 95,0%. A disponibilidade corresponde ao percentual de tempo, durante um período de 30 dias de operação, em que todos os serviços da solução estiveram em condições normais de funcionamento;

11.5.1.4. Mensalmente, deverá ser calculado o percentual de disponibilidade das soluções, com base na seguinte fórmula:

D = [(43200-Ti)/43200]*100, onde:

• D= Percentual de disponibilidade

• Ti= Somatório dos minutos em que foram observadas inoperâncias em quaisquer dos serviços contemplados pela solução de segurança de perímetro durante o período de faturamento (30 dias);

11.5.1.5. Sempre que forem apurados percentuais de disponibilidade que estejam abaixo do limite mínimo estabelecido (95%), serão aplicadas as penalidades previstas no Edital e seus Anexos.

11.5.2. Para o Serviço de Suporte Técnico:

11.5.2.1. Os serviços de suporte técnico serão prestados vinte quatro (24) horas por dia, sete (7) dias por semana.

11.5.2.2. Os serviços de suporte técnico serão acionados a partir da queda, falha ou registro de indisponibilidade gerado pelo monitoramento (quando for o caso) e/ou por meio de abertura de chamado a critério da equipe técnica do CONTRATANTE. Esses chamados serão classificados conforme as severidades especificadas a seguir:

• Severidade **ALTA**: Esse nível de severidade é aplicado quando há indisponibilidade na solução ou em qualquer serviço que a compõe; para a criação/configuração de políticas nos firewalls; para aplicação de ações de respostas a ataque. Prazo para início do atendimento: 2 horas

• Severidade **MÉDIA**: Esse nível de severidade é aplicado para solicitações de criação/configuração de políticas nos demais serviços que compõem a solução; quando há problema, simultâneo ou não, nos elementos que compõem os serviços/solução, embora ainda estejam disponíveis. Prazo para início do atendimento: 4 horas

• Severidade **BAIXA**: Esse nível de severidade é aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados. Prazo para início do atendimento: 10 horas

11.5.2.3. Faculta-se à CONTRATADA substituir temporariamente o equipamento, peça e componente defeituoso por outros de mesmas características técnicas, quando então, a partir de seu pleno estado de funcionamento, ficará suspensa a contagem do prazo de solução definitiva;

11.5.2.4. O prazo máximo para a substituição temporária será de 30 (trinta) dias, sendo que neste prazo o equipamento, peça e componente substituído deverá ser devolvido à CONTRATANTE em pleno estado de funcionamento ou ser substituído definitivamente;

11.5.2.5. A CONTRATADA deverá substituir, no prazo máximo de 10 (dez) dias úteis, qualquer equipamento, peça e componente que venha a se enquadrar em, pelo menos, um dos seguintes casos:

• Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;

• Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias.

• No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se à CONTRATADA promover a sua substituição em caráter definitivo;

• A substituição definitiva será admitida com anuência do CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, peça e componente ofertado, em relação àquele que está sendo substituído;

11.5.2.6. A CONTRATADA tornará disponíveis informações sobre desempenho e falhas (indisponibilidade) da solução de forma interativa (“on-line”), a partir do início do Período de Funcionamento Experimental (PFE);

11.5.2.7. Quando da ocorrência de falhas que tornem o serviço/solução indisponível por mais de 30 (trinta) minutos, a CONTRATADA deverá entregar à CONTRATANTE, juntamente com o relatório técnico mensal, a descrição detalhada da ocorrência, suas causas e as ações corretivas realizadas para tornar o serviço/solução novamente disponível;

11.5.2.8. A CONTRATADA deverá manter registro dos eventos, que porventura tenham provocado interrupções na solução dentro do período do faturamento mensal, de modo a justificar à CONTRATANTE a não consideração de tempos de inoperância, causados por falta de energia elétrica nas dependências do CONTRATANTE, por ações ou solicitações do CONTRATANTE ou ainda por manutenções programadas;

11.5.2.9. A CONTRATADA somente poderá efetuar manutenção técnica na solução e seus componentes após aprovação por parte do CONTRATANTE. Caso a manutenção seja efetuada sem essa aprovação, será considerado como indisponibilidade;

11.5.2.10. Será considerado o **Prazo de Solução Definitiva** como o tempo decorrido entre o registro de um chamado e a solução definitiva para efeito dos níveis exigidos.

11.5.2.11. Os chamados de severidade ALTA poderão ser atendidos on-site, a critério do CONTRATANTE. É vedado a CONTRATADA interromper o atendimento até que o serviço seja efetivamente recolocado em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. A interrupção do suporte técnico de um chamado desse tipo de severidade por parte da CONTRATADA e que não tenha sido previamente autorizado pelo CONTRATANTE, poderá ensejar em aplicação de penalidades previstas;

11.5.2.12. Após concluído o suporte técnico e com o serviço efetivamente recolocado em pleno estado de funcionamento, a CONTRATADA comunicará o fato à equipe técnica do CONTRATANTE e solicitará autorização para o fechamento do chamado. Caso o CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até o momento em que o serviço seja efetivamente recolocado em pleno estado de funcionamento pela CONTRATADA. Nesse caso, o CONTRATANTE fornecerá por e-mail, telefone ou através da interface de gerenciamento as pendências relativas ao chamado aberto;

11.5.2.13. Caso não haja manifestação dentro do prazo estipulado para o chamado em questão ou caso o CONTRATANTE entenda serem improcedentes as justificativas apresentadas, será iniciado processo de aplicação de penalidades previstas, conforme o nível de serviço transgredido.

11.5.2.14. O CONTRATANTE encaminhará à CONTRATADA, quando da reunião de alinhamento de expectativas, relação nominal de até 10 usuários que terão login e senha com perfis de acessos distintos aos serviços que compõem a solução bem como para abrir chamados. Esses perfis serão criados a critério do CONTRATANTE e configurados pela CONTRATADA;

11.5.2.15. Ao detectar tentativas de ataques à rede interna do CONTRATANTE ou aos serviços disponíveis em seu ambiente, a CONTRATADA deverá adotar, de imediato, as medidas de combate ao ataque independentemente das que forem estabelecidas pelo CONTRATANTE. No caso dessas medidas implicarem interrupções e/ou descaracterização dos serviços em uso, a CONTRATADA deverá entrar em contato com o CONTRATANTE em, no máximo, 15 (quinze) minutos, para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las. O CONTRATANTE se responsabilizará por eventuais danos causados pela não autorização de ações recomendadas pela CONTRATADA.

11.5.2.16. Essa lista pode ser ajustada durante o período de vigência do contrato a título de adequação às necessidades do CONTRATANTE mediante anuência e aceite da CONTRATADA, sem ônus para o CONTRATANTE.

11.5.3. Pelo não cumprimento do índice mínimo de DISPONIBILIDADE previsto, serão aplicadas as penalidades previstas em Contrato.

11.6. Implantação e Homologação

11.6.1. A CONTRATADA deverá apresentar um Plano de Implantação que será avaliado e aprovado pela equipe técnica do CONTRATANTE;

11.6.2. O Plano de Implantação deve conter a descrição de, no mínimo:

11.6.2.1. Atividades a serem desenvolvidas, incluindo os testes, e seus respectivos cronogramas;

11.6.2.2. Políticas de configuração dos elementos da solução;

11.6.2.3. Topologia lógica para a solução;

11.6.2.4. Ações de rollback.

11.6.3. Todo o trabalho realizado deve seguir o especificado no Plano de Implantação;

11.6.4. A CONTRATADA deverá realizar toda a instalação dos produtos, incluindo a configuração das ferramentas e os testes da solução, sob supervisão do CONTRATANTE;

11.6.5. Toda instalação deverá ser acompanhada pela equipe técnica do CONTRATANTE;

11.6.6. A CONTRATADA será responsável por dimensionar a solução a ser adotada na rede do CONTRATANTE e definir sua topologia. Esta solução estará sujeita à análise e aprovação da equipe técnica do CONTRATANTE;

11.6.7. A solução apresentada não pode causar impacto no funcionamento da rede (por exemplo, lentidão na rede local, degradação no desempenho das estações de trabalho e servidores, entre outros), devendo ser transparente ao usuário;

11.6.8. Caso o dimensionamento feito pela CONTRATADA não apresentar desempenho satisfatório, baseado nas recomendações do fabricante e conforme exposto na alínea anterior, a solução deverá ser redimensionada sem ônus adicional para o CONTRATANTE, mesmo que o redimensionamento envolva adição/substituição de hardware e software;

11.6.9. Todos os técnicos envolvidos na instalação e configuração devem possuir conhecimentos técnicos aprofundados nos produtos que ficarem sob sua responsabilidade;

11.6.10. O CONTRATANTE irá entregar a CONTRATADA uma relação de todos os serviços de informática que deverão ser testados antes e depois da implementação da solução;

11.6.11. O CONTRATANTE junto com a CONTRATADA irá preparar um Plano de Testes onde estão descritos todos os testes a serem realizados a fim de verificar todas as funcionalidades dos produtos oferecidos e os serviços de informática que deverão estar em total disponibilidade, descritas neste Termo;

11.6.12. O Plano de Testes deve ser apresentado em forma de tabela a fim de facilitar o acompanhamento dos mesmos por parte do CONTRATANTE;

11.6.13. Na tabela mencionada na alínea anterior, deve-se incluir os resultados esperados para cada teste realizado;

11.6.14. Os procedimentos descritos no Plano de Testes serão realizados pela CONTRATADA após a instalação e configuração dos produtos. Esses testes serão acompanhados pela equipe técnica do CONTRATANTE;

11.6.15. Caso seja detectado qualquer problema nos testes, em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização dessas correções, os testes serão reiniciados;

11.6.16. Se todos os testes forem realizados com sucesso, os produtos serão considerados implantados e dar-se-á início ao Período de Funcionamento Experimental - PFE, com duração de sete (7) dias corridos.

11.6.17. Para a homologação da solução, será estabelecido pelo CONTRATANTE um PFE - Período de Funcionamento Experimental - para testar o perfeito funcionamento dos produtos, verificar suas funcionalidades, analisando sua aderência às especificações deste Edital e seus Anexos, bem como à Proposta da CONTRATADA, e a sua compatibilidade com a estrutura já existente no CONTRATANTE;

11.6.18. Os produtos devem estar funcionando de acordo com as recomendações do fabricante;

11.6.19. Caberá à CONTRATANTE o provimento de alimentação elétrica e das portas UTP para conexão à rede local;

11.6.20. A CONTRATADA deverá instalar toda a solução na Sede do CONTRATANTE em até 60 (sessenta) dias após a assinatura do contrato. Na reunião de Alinhamento de Expectativas, deverá ser apresentado pela CONTRATADA o Plano de Implantação para análise e aprovação da CONTRATANTE;

11.6.21. Sugestão de conjunto de políticas, regras e filtros a serem configurados nos serviços da solução de segurança de perímetro;

11.6.22. Sugestão de graus de classificação de severidade de incidentes e as respectivas medidas que sugere serem adotadas em resposta aos alertas emitidos pelos serviços administrados;

11.6.23. As sugestões deverão ser apresentadas para discussão durante a reunião e as configurações definitivas devem ser apresentadas no Plano de Implantação;

11.6.23.1. Durante a implantação, esse conjunto de políticas, regras e filtros poderão ser alterados conforme a necessidade do CONTRATANTE.

11.6.24. Durante o PFE, não deve ocorrer qualquer falha ou interrupção em qualquer uma das funcionalidades dos produtos fornecidos;

11.6.25. A homologação da solução será vinculada também à entrega da Documentação Técnica - DT, bem como ao Treinamento;

11.6.26. Caso haja qualquer falha ou interrupção em qualquer uma das funcionalidades, a CONTRATADA deverá efetuar as devidas correções e, após a realização destas correções, o PFE será continuado de onde parou.

11.6.27. Caso não haja qualquer falha ou interrupção novamente em qualquer uma das funcionalidades, a solução será considerada homologada.

11.6.28. Para a homologação da solução será emitido, em até três (3) dias úteis, Termo de Recebimento Definitivo;

11.6.29. Após o PFE, terá de ser apresentado um baseline de funcionamento normal, baseado nas recomendações do fabricante, para cada hardware/software que compõe a solução. Além disso, terão de ser apresentados relatórios periódicos contendo informações de desempenho, referentes a esses elementos, para que seja identificada com antecedência a necessidade de adição/substituição de hardware/software. Esses relatórios serão apresentados pela CONTRATADA;

11.6.30. Entende-se por baseline as características de funcionamento padrão dos produtos, identificadas após implementação e realização dos respectivos testes;

11.6.31. No baseline devem ser identificados os aspectos que caracterizam a degradação dos produtos (levando-se em consideração o desempenho, a utilização dos recursos, o throughput, entre outros) e que indicam, consequentemente, a necessidade de upgrade destes.

11.6.32. A solução e o suporte técnico deverão estar em plena operação e disponíveis à CONTRATANTE no prazo de, no máximo, 60 (sessenta) dias corridos e contados a partir da assinatura do Contrato;

11.6.33. Entende-se que o serviço está em plena operação e disponível quando ele está apto a receber o Termo de Recebimento Definitivo;

11.7. Reunião para Alinhamento de Expectativas

11.7.1. Deverá ser realizada uma reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus Anexos, e esclarecer possíveis dúvidas acerca da infraestrutura de TI do CONTRATANTE;

11.7.2. Deverão participar dessa reunião, no mínimo, o Gestor do Contrato, membro(s) da equipe técnica do CONTRATANTE, Interlocutor e membro(s) da equipe técnica da CONTRATADA;

11.7.3. A reunião realizar-se-á no CONTRATANTE em até 5 (cinco) dias úteis após a assinatura do Contrato, conforme agendamento efetuado pelo Gestor do Contrato;

11.8. Recebimento das Soluções

11.8.1. A CONTRATADA somente poderá dar início ao faturamento da solução após estar de posse do Termo de Recebimento Definitivo, emitido conforme condições estabelecidas no Edital e Termo de Referência.

11.9. Execução dos Serviços

11.9.1. O serviço deverá ser prestado nas dependências do CONTRATANTE.

11.9.2. Eventual solicitação de mudança de endereço será feita por meio de ofício.

11.10. Visita Técnica

11.10.1. A visita é opcional e servirá para que o interessado tome conhecimento detalhado das plataformas instaladas, dos locais de realização dos serviços, das instalações, das condições técnicas e ambientais, dos projetos em andamento, do parque de TI e dos procedimentos adotados para execução das tarefas que compõem os serviços objeto da licitação;

11.10.2. A visita técnica deverá ocorrer por horário marcado, e será agendada com o CONTRATANTE;

11.10.3. O agendamento de visita deverá ocorrer até 48 (quarenta e oito) horas antes da data e horário de abertura do processo licitatório;

11.10.4. A visita técnica deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas antes da abertura da licitação;

11.10.5. Durante a visita técnica, serão esclarecidas dúvidas da CONTRATADA e será dada ciência:

11.10.5.1. Dos locais onde deverão ser realizados os serviços contratados, como CPDs, ativos de redes, periféricos de apoio e setores de demanda e aprovação;

11.10.5.2. Dos modelos de equipamentos servidores, armazenadores, integradores e de comunicação objeto dos serviços e utilizados pelo CONTRATANTE;

11.10.5.3. Dos softwares, aplicativos e ferramentas auxiliares utilizadas pelo CONTRATANTE.

11.10.6. Não terão fundamento alegações posteriores de desconhecimento dos objetos e suas características de contratação, gestão e execução, sob pretexto da CONTRATADA não haver efetuado a visita técnica.

11.11. Treinamento

11.11.1. A CONTRATADA deverá transferir o conhecimento da Solução ofertada para uma equipe de técnicos da CONTRATANTE compreendendo as tecnologias envolvidas nos serviços contratados, assim como capacitação nos produtos e softwares utilizados para atender aos requisitos das especificações técnicas;

11.11.2. A CONTRATADA deverá apresentar, em até 20 (vinte) dias após assinatura do Contrato, um Plano de Treinamento que será avaliado e aprovado pela equipe técnica do CONTRATANTE;

11.11.2.1. O conteúdo programático da solução deve ser, minimamente, o mesmo praticado pelo fabricante;

11.11.2.2. O Treinamento deverá abordar cada uma das ferramentas, contemplando módulos, com conteúdo teórico e prático, com programas mínimos que abordem toda a instalação, configuração e utilização das mesmas;

11.11.2.3. O treinamento deverá contemplar atividades práticas. Para a consecução da parte prática, poderão ser utilizados equipamentos similares aos ofertados, além dos softwares que fazem parte da solução, ou os próprios equipamentos fornecidos, desde que o treinamento não cause impacto nas operações do ambiente do CONTRATANTE;

11.11.3. A CONTRATADA deverá preparar técnicos do CONTRATANTE na instalação, configuração e utilização de funcionalidades básicas e avançadas da solução, assim como realizar atividades de suporte (troubleshooting) para todos os equipamentos da solução, observada as seguintes condições:

11.11.3.1. É de responsabilidade da CONTRATADA assumir todas as despesas relativas a pessoal e quaisquer outras oriundas, derivadas ou conexas com a contratação, ficando, ainda, para todos os efeitos legais, declaradas pela CONTRATADA a inexistência de qualquer vínculo empregatício entre seus empregados e/ou prepostos e o CONTRATANTE.

11.11.3.2. A CONTRATADA deverá prover toda a estrutura para os treinamentos;

11.11.3.3. O CONTRATANTE poderá avaliar os treinamentos com meios próprios e, caso este seja julgado deficiente, a CONTRATADA deverá prover o devido reforço; Para que um treinamento seja considerado efetivo deverá ser considerado satisfatório por pelo menos 70% dos treinandos;

11.11.3.4. Ao CONTRATANTE deverá ser fornecido certificado de participação individual contendo conteúdo ministrado e hora/aula realizada;

11.11.3.4.1. Hora/aula mínima a ser ministrada nos treinamentos por solução e por turma:

11.11.3.4.1.1. NGFW: mínimo de 30h/a;
11.11.3.4.1.2. WAF: mínimo de 16h/a;
11.11.3.4.1.3. Segurança de Endpoint: mínimo de 16h/a;
11.11.3.4.1.4. Rede sem fio: mínimo de 8h/a;
11.11.3.4.1.5. Switch PoE: mínimo de 4h/a;
11.11.3.4.1.6. Gestão de Vunerabilidades: mínimo de 12h/a;

11.11.3.5. A CONTRATADA deverá ministrar treinamento modalidade teórico e "hands on" aos técnicos do CONTRATANTE para até 10 (dez) participantes, e deverá ser previsto duas turmas de treinamento para fins de distribuição da equipe do CONTRATANTE, sendo uma turma no período matutino e outra no período vespertino com duração de quatro (4) horas/aula por turma, por dia;

11.11.3.6. O facilitador designado pela CONTRATADA deverá ser profissional capacitado na solução implantada devendo possuir conhecimento suficiente para configurar, operar e prestar suporte técnico aos produtos contratados além de conhecimentos de rede e segurança em rede de dados.

11.11.3.7. O facilitador deverá ter experiência comprovada em ministrar os conteúdos solicitados;

11.11.3.8. O treinamento será realizado na sede da CONTRATANTE;

11.11.3.9. Todo material didático disponibilizado no treinamento deverá ser fornecido pela CONTRATADA e estarão inclusos no escopo do treinamento;

11.12. WORKSHOP DE ATUALIZAÇÃO DE CONHECIMENTOS

11.12.1.1. Deverão ser ministrados somente para as soluções de Sistema de Firewall de Nova Geração, Sistema de Firewall de Aplicação Web – WAF, Sistema de Segurança para Endpoint e Sistema de Gestão Contínua de Vulnerabilidades

11.12.1.2. A Contratada deverá realizar 4 (quatro) Workshops de atualização de Conhecimentos, para até 10 (dez) servidores da Contratante.

11.12.1.3. Cada workshop deverá ser concluído até 90 (noventa) dias corridos após a data de término de cada ciclo anual do contrato, considerando a data de assinatura do contrato como o início do primeiro ciclo anual, de acordo com cronograma estabelecido entre a Equipe Técnica da Contratante.

11.12.1.4. Os Workshops deverão ser realizados nas dependências da Contratante, e deverão ser ministrados por instrutores preparados e certificados pelo fabricante dos produtos.

11.12.1.5. O cronograma para realização dos workshops deverá ser proposto pela Contratada, até 30 (trinta) dias corridos após o término de cada ciclo anual do contrato, considerando a data de assinatura do contrato como o início do primeiro ciclo anual. A Contratante analisará o cronograma, estabelecendo posteriormente, em até 5 (cinco) dias úteis, as datas definitivas com a Contratada.

11.12.1.6. Os workshops deverão ter carga horária mínima de 8 (oito) horas, cobrindo conteúdo teórico e prático, em nível avançado e personalizado para a solução fornecida, com foco nas atualizações aplicadas à solução durante cada ciclo anual, bem como em tópicos de interesse da Equipe Técnica da Contratante.

11.12.1.7. O workshop e o material didático deverão estar, preferencialmente, em língua portuguesa, ou, na sua impossibilidade, em língua inglesa.

11.12.1.8. Caso os treinamentos sejam realizados fora da Sede da Contratante, despesas com transporte (aéreo e local), hospedagem e alimentação deverão ser custeadas pela Contratada.

11.12.1.9. Os workshops serão avaliados por cada grupo, e caso não sejam considerado satisfatório por pelo menos 70% dos treinandos, fica a Contratada obrigada a realizar novo workshop, dentro de 30 (trinta) dias corridos, sem ônus adicional para a Contratante, corrigindo as deficiências apontadas na avaliação.

11.12.1.10. Deverão ser emitidos certificados de conclusão dos workshops para todos os participantes. O prazo para emissão e envio dos certificados aos alunos é de 30 (trinta) dias corridos após o término de cada curso.

11.12.1.11. Após a realização de cada workshop, será emitido um Termo de Aceite do Workshop de Atualização e Conhecimentos, em até 15 (quinze) dias corridos a contar da conclusão de cada workshop.

12. CARACTERÍSTICAS TÉCNICAS

12.1. Características Gerais

12.1.1. Os serviços e sistemas deverão ser implementados sobre uma infraestrutura de hardware e software de uso exclusivo do CONTRATANTE e dedicada para esta finalidade, do tipo *appliance* e *access points wireless*, projetados especificamente para as funcionalidades propostas, não sendo admitidas soluções baseadas em computadores de uso geral, devendo a empresa fornecer o cabeamento, adaptadores e demais conexões necessárias para a completa conectividade dos recursos empregados à infraestrutura do CONTRATANTE;

12.1.2. As soluções de NGFW, WAF e Segurança de Endpoint, por terem a finalidade de proteger o ambiente tecnológico da CONTRATADA que está exposto em toda rede mundial de computadores; por ser mais um item de averiguação técnica das soluções, certificando que passaram pelo crivo de organização especializada; e por não inviabilizar o certame, pelo rol de fabricantes que possuem tais certificações, deverão apresentar ao menos uma das seguintes certificações, **ou outra equivalente**:

12.1.2.1. ICSA labs, NSS labs, Common Criteria.

12.1.3. Esses equipamentos deverão ser instalados e configurados pela CONTRATADA nas instalações físicas e lógicas da rede do CONTRATANTE, na qual a CONTRATADA declara conhecer;

12.1.4. As soluções de Firewall de Nova Geração (NGFW) e WAF devem trabalhar em alta disponibilidade, ou seja, para cada *appliance* que compuser a solução, deverá ser ofertado *appliance* de funcionalidades idênticas, de forma que funcione com modelo de alta disponibilidade e tolerante a falhas. Os pares de *appliance* deverão trabalhar no tipo ATIVO/ATIVO com licenciamento, todas as funções ativas, independente da falha de um dos elementos que compõem este par.

12.1.5. As funcionalidades requisitadas para o NGFW poderão ser atendidas por qualquer módulo/recurso dos *appliances.*

12.1.6. Não serão aceitas soluções baseadas em PC de uso geral, soluções que contenham componentes do tipo acionadores de discos rígidos, soluções dos tipos/linhas "*home", "free*" e "community" e soluções que não utilizem as versões mais completas das bases de dados/assinaturas e funcionalidades dos fabricantes. Os dois dispositivos são ligados em paralelo, com réplicas do estado de conexões entre eles.

12.1.7. A solução provida deverá suportar:

12.1.7.1. As interfaces de rede LAN devem, cada uma, suportar tráfego de no mínimo 1 Gbps Full Duplex;

12.1.7.2. Recurso de backup das configurações que deverá ser efetivado de forma automática e enviado para um ambiente separado da solução;

12.1.8. Os equipamentos que compõem a solução deverão ter seu funcionamento restrito às suas funções, não podendo interferir ou causar lentidão no funcionamento da rede local do CONTRATANTE.

12.1.9. Devem ser fornecidos todos os GBICs e SFPs necessários para o atendimento de todos os itens solicitados.

12.1.10. O software e o hardware empregados deverão corresponder a uma solução de notória eficácia já em uso no mercado nacional, devendo ser dimensionados e configurados de forma que não prejudique o desempenho da infraestrutura da rede do CONTRATANTE e seus serviços;

12.1.10.1. A solução deve suportar autenticação LDAP, RADIUS e ser totalmente integrada com Microsoft Active Directory 2003, 2008, 2012 e superiores;

12.1.11. A CONTRATADA deverá fornecer à CONTRATANTE acesso de leitura às configurações da solução;

12.1.12. Os equipamentos deverão possuir robustez adequada ao tráfego de dados do CONTRATANTE;

12.1.13. Os equipamentos deverão ser bivolt ou fornecidos com transformadores para atender ao requisitado pela CONTRATANTE quanto à voltagem.

12.2. Sistema de Firewall de Nova Geração (NGFW)

12.2.1. Atender ao especificado no item **12.1.2** e subitem(s), quanto aos certificados.

12.2.2. Sistema de Firewall de Nova Geração (NGFW) – TIPO A

12.2.2.1. Cada *appliance* deve suportar em ambiente de produção (mundo real), no mínimo, **200 (duzentos) Mbps** de throughput de firewall de tráfego inspecionado SSL e minimamente as funcionalidades de firewall, controle de aplicação, webfilter, antivírus de gateway e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante.

12.2.2.2. Se o fabricante não possuir a informação de throughput requerida no item anterior, deverá se enquadrar em uma das seguintes situações em ambiente de produção:

12.2.2.2.1. Suportar em ambiente de produção, no mínimo, **300 (trezentos) Mbps** de throughput de firewall com tráfego inspecionado SSL e minimamente as funcionalidades de antivírus de gateway e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante;

12.2.2.2.2. Suportar em ambiente de produção, no mínimo, **300 (trezentos) Mbps** de throughput de firewall minimamente com as funcionalidades de controle de aplicação, antivírus de gateway e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante;

12.2.2.2.3. Suportar em ambiente de produção, no mínimo, **400 (quatrocentos) Mbps** de throughput de firewall minimamente com as funcionalidades de controle de aplicação, webfilter e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante;

12.2.2.3. Entende-se por ambiente de produção, a informação apresentada no *datasheet* do fabricante como throughput de mundo/ambiente real, ou documentação que contenha mensuração por organização/empresa reconhecida por ser especialista nesse tipo de análise e disponibilizada oficialmente no sítio ou *datasheet* do fabricante, e que também contenha o throughput de mundo/ambiente real/corporativo.

12.2.2.4. Permitir montagem em rack com largura padrão de 19 polegadas. Deverão ser fornecidos todos os cabos, suportes (se necessários, "gavetas", "braços" e "trilhos") para a instalação dos equipamentos no rack.

12.2.2.5. Cada equipamento deve possuir dimensão de 1U.

12.2.2.5.1. Não serão aceitos equipamentos do tipo desktops com kits adaptáveis a rack;

12.2.2.6. Cada *appliance* deve ser fornecido com, no mínimo, 4 (quatro) interfaces Gigabit Ethernet.

12.2.2.7. Cada *appliance* deve ser fornecido com, no mínimo, 2 (duas) interfaces SFP 1Gbps juntamente com os cabos e conectores.

12.2.2.8. Cada appliance deve suportar no mínimo 90.000 (noventa mil) conexões por segundo.

12.2.3. Sistema de Firewall de Nova Geração (NGFW) – TIPO B

12.2.3.1. Cada *appliance* deve suportar em ambiente de produção, no mínimo, **70 (setenta) Mbps** de throughput de firewall de tráfego inspecionado SSL e minimamente as funcionalidades de firewall, controle de aplicação, webfilter, antivírus de gateway e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante.

12.2.3.2. Se o fabricante não possuir a informação de throughput requerida no item anterior, deverá se enquadrar em uma das seguintes situações em ambiente de produção:

12.2.3.2.1. Suportar em ambiente de produção, no mínimo, **100 (cem) Mbps** de throughput de firewall com tráfego inspecionado SSL e minimamente as funcionalidades de antivírus de gateway e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante.

12.2.3.2.2. Suportar em ambiente de produção, no mínimo, **100 (cem) Mbps** de throughput de firewall minimamente com as funcionalidades de firewall, controle de aplicação, antivírus de gateway e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante.

12.2.3.2.3. Suportar em ambiente de produção, no mínimo, **130 (cento e trinta) Mbps** de throughput de firewall minimamente com as funcionalidades de controle de aplicação, webfilter e IPS habilitadas com todas as assinaturas recomendadas pelo fabricante

12.2.3.3. Entende-se por ambiente de produção, a informação apresentada no *datasheet* do fabricante como throughput de mundo/ambiente real, ou documentação que contenha mensuração por organização/empresa reconhecida por ser especialista nesse tipo de análise e disponibilizada oficialmente no sítio ou *datasheet* do fabricante, e que também contenha o throughput de mundo/ambiente real/corporativo.

12.2.3.4. Cada *appliance* deve ser fornecido com, no mínimo, 5 (cinco) interfaces Gigabit Ethernet LAN.

12.2.3.5. Cada appliance deve suportar no mínimo 20.000 (vinte mil) conexões por segundo.

12.2.4. Principais características dos firewalls dos tipos A e B:

12.2.4.1. Firewall

12.2.4.2. IPS/IDS

12.2.4.3. VPN

12.2.4.4. WebFilter

12.2.4.5. Application Control

12.2.4.6. Controle de acesso convidado (Captive Portal)

12.2.4.7. Redundância de links de conexão de internet

12.2.4.8. Balanceamento de Carga

12.2.4.9. Proteção contra explorações na camada de aplicativos que atingem os servidores;

12.2.4.10. Conectividade e acesso remoto por VPN, IPSec e SSL VPN;

12.2.4.11. Fornecer primeira camada de defesa contra vírus, cavalos de tróia, keyloggers e outros tipos de malware;

12.2.4.12. Proteção contra conteúdo da web inadequado, ilegal e perigoso através da filtragem de conteúdo e URL;

12.2.4.13. Verificação de vários tipos de aplicativos e protocolos para proteger contra ameaças internas e externas;

12.2.4.14. Trabalha na redução de latência para preservar a largura de banda e otimizar desempenho;

12.2.4.15. Relatórios analíticos relativos a tráfego de aplicativos, uso de largura de banda e de ameaças à segurança;

12.2.5. A solução de firewall deve ser uma solução integrada composta de Hardware e Software de segurança da informação do tipo NGFW (Next Generation Firewall) que tenha a capacidade de integrar em um único dispositivo: filtro de pacotes com controle de estado, controle de aplicações, camada de antivírus de gateway, filtro de conteúdo WEB, VPN, IDS/IPS, balanceamento de carga e QoS, em um esquema de alta disponibilidade (dois equipamentos funcionando de forma que se um pare o outro assuma as funções do equipamento que parou);

12.2.6. A solução deve possuir a capacidade de reconhecimento de aplicações - ter visibilidade das aplicações e aplicar políticas de segurança na camada de aplicação independente de porta ou protocolo, prevenção de ameaças e controle granular de permissões.

12.2.7. A comprovação dos dados de throughput exigidos se dará através de documento público localizado no site do fabricante, ou documento emitido pelo **fabricante**, destinado à CONTRATANTE e publicado em seu site oficial, informando o modelo do produto e o atendimento do mesmo às exigências deste edital, detalhando os dados de desempenho obtidos e respectivas referências.

12.2.8. Proteção e prevenção contra ataques de dia zero.

12.2.9. Deve permitir o controle de acesso convidado (Captive Portal).

12.2.10. O serviço deve possibilitar a implementação de políticas de segurança orientadas a credenciais de usuários através de autenticação LDAP, RADIUS e totalmente integrado com Microsoft AD 2003, 2008 2012 e superiores, independentemente do endereço IP de origem;

12.2.11. Permitir a filtragem de pacotes através da análise do endereço de origem, endereço de destino e protocolo;

12.2.12. Obedecer à marcação prévia de QoS; e capacidade de trabalhar em layer 3 (roteando) ou layer 2 (em bridge);

12.2.13. Suportar tráfego de IP Multicast;

12.2.14. Implementar Network Address Translation (NAT) e Port Address Translation (PAT);

12.2.15. Possuir a capacidade de tomar a decisão de encaminhar ou bloquear um pacote, com base nos pacotes anteriores (stateful inspection);

12.2.16. Possuir filtro de aplicações, de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (bloqueio, liberação ou redução/aumento de banda) de aplicações do tipo peer-to-peer, mensageria instantânea e download de arquivos;

12.2.17. Suportar tráfego VoIP e os padrões SIP e H.323;

12.2.18. Compatível com redes IPv4, IPv6 e redes híbridas, devendo estar em conformidade com as RFC-s pertinentes;

12.2.19. Permitir o controle de acesso por usuário, para todas as plataformas com browser através de autenticação via formulário para todos os serviços suportados, de forma que um determinado usuário tenha seu perfil de acesso automaticamente configurado;

12.2.20. Possuir perfis de acesso hierárquicos;

12.2.21. Prover mecanismo que permita a especificação da validade para regras de filtragem, individualmente (por regra), por dia da semana e horário; e permitir a visualização pela interface gráfica, em tempo real, de todas as conexões TCP e sessões UDP ativas através do dispositivo e a finalização de qualquer uma destas sessões ou conexões;

12.2.22. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em dado momento;

12.2.23. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;

12.2.24. Possuir mecanismo que permita capturar o tráfego de rede em tempo real (sniffer) via interface gráfica, com visualização em tempo real pela interface gráfica e com capacidade para exportação dos dados capturados para arquivo no mínimo em formato PCAP;

12.2.25. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

12.2.26. Prover proteção contra os ataques de negação de serviço SYN Flood, Land, Tear Drop e Ping ODeath;

12.2.27. Permitir visualização dos sites acessados em tempo real;

12.2.28. Permitir a inserção de uma URL de redirecionamento para bloqueio por palavras-chave nas regras de perfil para HTTP ou FTP e tipos de arquivos bloqueados;

12.2.29. Permitir a filtragem de URL-s, para os protocolos HTTP, HTTPS, FTP, por usuário, permitindo a definição de perfis de acesso diferenciados para cada usuário ou grupo;

12.2.30. Permitir que VPN-s cliente-servidor sejam estabelecidas com o dispositivo, de forma transparente, e então redirecionadas para qualquer servidor interno da rede, sem o uso de cliente de criptografia específico e com autenticação opcional de usuários via certificados digitais padrão X.509;

12.2.31. Realizar controle, inspeção e descriptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

12.2.32. Deve realizar offload de certificado em inspeção de conexões SSL de entrada (Inbound).

12.2.33. Deve descriptografar tráfego Inbound e Outbound em conexões negociadas com mínimo TLS 1.2.

12.2.34. Permite identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Skype e ataques mediante a porta 443;

12.2.35. Suportar a detecção de aplicações dinâmicas dentro de sessões HTTP;

12.2.36. Prover serviço VPN (Virtual Private Network) para pacotes IP e VPN SSL, com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPN-s através da Internet;

12.2.37. Suportar padrão IPSEC, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;

12.2.38. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

12.2.39. Possibilitar mecanismo de criação de VPN-s entre máquinas Windows 7, Windows 8, Windows 10, Linux e Mac OS e o dispositivo, com chaves de criptografia simétricas com tamanho igual ou superior a 128 bits;

12.2.40. Funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs das redes internas, colocando-os, virtualmente, dentro das mesmas (0 hops);

12.2.41. Prover cliente VPN para as plataformas Windows 7, Windows 8, Windows 10, Linux e Mac OS, que permita uso de chaves criptográficas simétricas com 128 ou mais bits;

12.2.42. Deverá ser possível configurar o endereço/range IP a ser atribuído a placa de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;

12.2.43. No VPN cliente/firewall deverá ser possível a configuração do envio ou não de pacotes broadcast da rede onde o servidor se encontra para o cliente;

12.2.44. O cliente de VPN deverá possibilitar que seu funcionamento seja sincronizado ou não com o dial-up do Windows, possibilitando que ele estabeleça a VPN automática e imediatamente depois de se ter estabelecido uma conexão discada;

12.2.45. Suportar VPN Failover (reestabelecimento da VPN sobre um segundo enlace caso haja falha no enlace principal);

12.2.46. A solução de VPN deverá trabalhar no mínimo com os seguintes protocolos: IPSEC, L2TP, SSL;

12.2.47. Possuir funcionalidade Dead Peer Detection (DPD), ou similar;

12.2.48. Prover funcionalidade de VPN SSL, com o estabelecimento do túnel VPN e autenticação via browser;

12.2.49. Disponibilidade de Software SSL-Client para no mínimo: Windows 7, Windows 8, Windows 10, Linux e Mac OS;

12.2.50. Possibilitar drag-and-drop (arrastar e soltar) para criação e alteração de regras, por meio da interface gráfica;

12.2.51. A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos dispositivos sem a necessidade de se executar várias interfaces;

12.2.52. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do dispositivo, incluindo a configuração de VPN-s, NAT, perfis de acesso e regras de filtragem;

12.2.53. Possuir mecanismo que permita a realização de cópias de segurança (backups) e restauração remota.

12.2.54. Deverá ser capaz de executar um backup por linha de comando e oferecer a opção de salvar o arquivo de backup localmente ou exportar usando o protocolo FTP;

12.2.55. Suportar o uso simultâneo de múltiplos links em um mesmo firewall (poderia ser appliance), de provedores distintos ou não, sendo o firewall o responsável por dividir o tráfego entre os distintos links;

12.2.56. Permitir o balanceamento de links.

12.2.57. Implementar mecanismo de balanceamento de carga, permitindo com que vários servidores internos, sejam acessados externamente pelo mesmo endereço IP. O balanceamento de canal deverá monitorar os servidores internos e, em caso de queda de um destes, dividir o tráfego entre os demais, automaticamente;

12.2.58. Implementar mecanismo de persistência de sessão para o balanceamento de carga, através de diversas conexões, para quaisquer protocolos suportados pelos servidores sendo balanceados;

12.2.59. Permitir inspeção de pacotes à nível de aplicativo;

12.2.60. Deve ser capaz liberar e bloquear de conexões e aplicativos através de análise DPI (Deep Packet Inspection) ou similiar utilizando aplicações cadastradas para aplicações de Firewall com fornecimento das assinaturas de aplicações e possibilidade de adição das mesmas manualmente em caso de necessidade.

12.2.61. A solução deverá suportar a implantação de zona desmilitarizada (DMZ), além dos segmentos de rede externa e interna;

12.2.62. Deverá suportar dois canais de comunicação com a Internet de no mínimo 50 Mbps cada, de operadoras distintas, de maneira simultânea, garantindo alta disponibilidade;

12.2.63. Deverá possuir sincronismo entre as configurações como Regras de Firewall, Regras de NAT, Entidades, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmicas, Perfis e bases de antivírus, filtros web e IDS/IPS.

12.3. CONSOLE DE GERÊNCIA CENTRALIZADO

12.3.1. A solução de gerência deverá ser separada do Gateway de segurança onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto assim como logs e relatórios de forma unificada;

12.3.2. Centralizar a administração de regras e políticas do(s) cluster(s), usando uma única interface de gerenciamento;

12.3.3. Implementar gerenciamento centralizado das licenças de utilização da solução, incluindo adição e remoção de licenças;

12.3.4. A solução de gerência centralizada deverá ser composta por uma console de gerenciamento;

12.3.5. Deverá permitir administração via interface gráfica e linha de comando (CLI) utilizando protocolo seguro de comunicação;

12.3.6. A gerência deve possuir console de Log onde deve ter a capacidade de visualizar os logs de segurança em tempo real permitindo ao administrador realizar as devidas análises para fins de troubleshooting;

12.3.7. A solução de gerência, deverá prover fácil administração na aplicação das políticas para os Gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança, onde pode ser aplicada nos Gateways remotos.

12.3.8. Solução deve incluir o status de todos os túneis VPN.

12.3.9. A solução deverá prover informações gerais de cada gateway como volume de pacotes aceitos, conexões concorrentes e novas conexões;

12.3.10. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows;

12.3.11. A solução de gerência centralizada deverá possuir capacidade de analisar logs e eventos com intuito de mitigar qualquer anomalia no ambiente independente do appliance de segurança estar sob ataque ou elevado consumo de CPU e memória;

12.3.12. Permitir nas regras de Firewall, Controle de Aplicação e URL a ação “exceção”.

12.3.13. A solução deve ser capaz de criar regras de exceção para determinado tipo de proteção;

12.3.14. O gerenciamento deve permitir:

12.3.14.1. Criação e administração de políticas de Firewall, Controle de aplicação e IPS;

12.3.14.2. Criação e administração de políticas de Antivírus e Anti-Malware;

12.3.14.3. Criação e administração de políticas de Filtro de URL e prevenção contra ameaças avançadas;

12.3.14.4. Criação e administração de políticas de VPNs IPSec e SSL;

12.3.14.5. Monitoração de logs;

12.3.14.6. Ferramentas de investigação de logs;

12.3.14.7. Debugging;

12.3.14.8. Captura de pacotes;

12.3.15. Acesso concorrente de administradores;

12.3.16. Deve possuir mecanismo para facilitar identificação de regras;

12.3.17. Definição de perfis de acesso à console com permissões granulares.

12.3.18. Deve atribuir sequencialmente um número a cada regra de Firewall, NAT e QoS;

12.3.19. Backup das configurações e rollback de configuração para a última configuração salva;

12.3.20. Suportar Rollback de Sistema Operacional para a última versão local;

12.3.21. Validação de regras antes da aplicação;

12.3.22. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

12.3.23. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

12.3.24. Deve ser possível exportar os logs;

12.3.25. Gerar alertas automáticos minimamente via e-mail e SNMP;

12.3.26. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelo equipamento gerenciado;

12.3.27. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deverá possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível/homologado com/para VMware;

12.3.28. Permitir que todas as alterações em objetos e objetos gerem log de auditoria;

12.3.29. A solução deve pemitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;

12.3.30. A solução deve vir pré-configurada com melhores práticas para regras de: Proteção contra Bots, Anti-Spam, Anti-vírus, Controle de Aplicação, Prevenção de vazamento de informações, Firewall, Sistema Operacional do Gateway de Segurança, Identificação de usuários, IPS, VPN Site-to-Site, VPN Client-to-Site, Emulação de arquivos e Controle de navegação Web;

12.4. Sistema de Prevenção Contra Intrusão (IPS)

12.4.1. A solução de Prevenção Contra Intrusão em software do tipo IDS/IPS e Filtro de Aplicações deve funcionar integrada ao Sistema de Firewall de Nova Geração (NGFW) e prover capacidade de integrar em um único dispositivo: Inspeção de trafego de modo passivo e ativo e filtragem de aplicações;

12.4.2. Operar baseado em um banco de dados da própria solução que contenha os padrões de ataques (assinaturas) já conhecidos e identificados, descrevendo as ações normalmente praticadas com intenções maliciosas e/ou suspeitas;

12.4.3. Ser dimensionado e configurado de forma que não afete o desempenho da infraestrutura de rede como um todo e deve ser capaz de armazenar os resultados da sua execução (logs) em um banco de dados da própria solução que permita à CONTRATANTE a realização de consultas on-line;

12.4.4. Possuir as assinaturas de detecção e prevenção baseadas em vulnerabilidades, permitindo a detecção de ataques desconhecidos ou variantes de ataques sem a necessidade de assinaturas específicas;

12.4.5. Permitir que as assinaturas de detecção e prevenção sejam associadas a grupos de servidores específicos;

12.4.6. Implementar reconhecimento de padrões de ataque;

12.4.7. Implementar detecção de anomalias;

12.4.8. Implementar decodificação de múltiplos formatos de Unicode;

12.4.9. Suportar fragmentação e desfragmentação IP;

12.4.10. Deverá permitir atuar nos seguintes modos: IDS: Está modalidade simplesmente detecta o ataque e permite a visualização e geração de logs;

12.4.10.1. Modo IDS/IPS passivo e ativo permitindo a analise o trafego da rede de encontro a regras definidas pelo usuário, executando diversas ações baseadas em suas regras;

12.4.10.2. IPS em Modo Aprendizado: Deverá funcionar da mesma forma que o modo de operação anterior (IPS), mas não poderá executar nenhuma ação de prevenção. Este modo informa ao usuário quais pacotes poderiam ter sido bloqueados. Este modo é recomendado para testes em ambientes para redução de falsos positivos.

12.4.10.3. Deve operar em camada 2 OSI (Layer 2), span-mode ou bridge-mode (segmento), sendo vedada a alocação de IP válido nas interfaces físicas de rede.

12.4.11. Possuir modo de Inspeção baseado em regras e assinaturas;

12.4.12. Metodologias de detecção Multidimensional:

12.4.12.1. Assinaturas (Impressões Digitais) do Ataque.

12.4.12.2. Anomalias no Protocolo.

12.4.12.3. Anomalias no Comportamento.

12.4.13. A base de assinaturas do sistema de IPS e DPI nativo (ou similar) deverá ser fornecida pelo período do contrato conforme Item "Garantia" e "Atualizações e Assinaturas";

12.4.14. Possuir filtro de aplicações de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (auditoria, geração e alertas, bloqueios e liberação) serviços bem como de aplicações do tipo peer-to-peer, de download de arquivos, entre outros;

12.4.15. Deverá permitir que as assinaturas de detecção e prevenção sejam associadas a grupos de servidores específicos;

12.4.16. Deverá suportar fragmentação e desfragmentação IP;

12.4.17. Deverá implementar detecção de protocolos independentemente da porta utilizada;

12.4.18. Deverá possibilitar a resposta há eventos com TCP Reset ou descarte de pacotes

12.4.19. Prover proteção contra os ataques de negação de serviço SYN Flood, Land, Tear Drop e Ping ODeath;

12.4.20. Possuir sistema de prevenção de intrusão (IPS) nativo, permitindo o bloqueio do ataque em caso de detecção do mesmo;

12.4.21. Usar autenticação forte e mecanismos de criptografia para todos os componentes da solução;

12.4.22. Remontar todos fluxos de pacote fragmentados ou não;

12.4.23. Deverá suportar o conceito de pré-processador, permitindo que um determinado protocolo funcione apenas em um conjunto de portas. Este conceito pode ser utilizado nos proxies que tem portas dinâmicas como: RPC, FTP, SIP, H323. Assim, as regras destes protocolos não seriam aplicadas em todas as portas e conexões, seriam aplicadas apenas nas conexões negociadas, economizando CPU;

12.4.24. Fabricante deve garantir o fornecimento de updates diários dentro do período de assinatura contratado;

12.4.25. Deverá permitir a atualização automática das assinaturas por meio de agendamento diário;

12.4.26. Prover linguagem para criação de regras proprietária ou compatível com assinaturas do Snort;

12.4.27. Deverá ser possível importar regras compatíveis do padrão do Snort;

12.4.28. Deve implementar proteção positiva e segura contra:

12.4.28.1. Ataques de Worm, Trojan, Backdoors, Portscans, IP Spoofing, DoS e Spywares;

12.4.28.2. Ataques a comunicações VoIP;

12.4.28.3. Ataques e utilização de tecnologia P2P;

12.4.28.4. Ataques de estouro de pilha (buffer overflow);

12.4.28.5. Ataques do tipo dia-zero (zero-day);

12.4.28.6. Tráfego mal formado;

12.4.28.7. Cabeçalhos inválidos de protocolo;

12.4.29. Deve possuir filtros de normalização de tráfego, que bloqueiem tráfego malicioso ou que apresente comportamento anormal.

12.4.30. Possuir capacidade de inspeção profunda de pacotes (Deep Package Inspection - DPI) ou similar, incluindo todo o payload.

12.4.31. Possuir capacidade de inspecionar e bloquear em tempo real, aplicativos e transferências de arquivos do tipo P2P (peer to peer) e de IM (Instant Messaging);

12.4.32. Possuir a capacidade de controlar, bloquear o download de tipos de arquivos específicos via FTP e HTTP;

12.4.33. Permitir o controle de acesso por fluxo de tráfego para controle de IMs como Skype, Google Talk, Yahoo Messenger e Facebook Messenger;

12.4.34. Possui a capacidade de identificar o tráfego Web e classifica-lo de acordo com as aplicações e sub aplicações trafegando na rede, tais como redes sociais: Facebook, Google+, Twitter, etc; de comunicação: Skype, Gmail, GTalk, MSN, etc;

12.4.35. Permitir identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Ultrasurf, Skype e ataques mediante a porta 443;

12.4.36. Suporta a detecção de aplicações dinâmicas dentro de sessões HTTP;

12.5. Sistema de Filtro de Conteúdo Web (Webfilter)

12.5.1. A solução de Filtro de Conteúdo Web deve funcionar integrada ao Sistema de Firewall de Nova Geração (NGFW).

12.5.2. Ser dimensionado e configurado de forma a armazenar os resultados da sua execução (logs) em um banco de dados da própria solução que permita à CONTRATANTE a realização de consultas on-line;

12.5.3. Ser integrado à infraestrutura de rede existente, depois de fornecidas algumas configurações básicas de IP (endereço, gateway, servidor de DNS etc.), implementando as políticas de acesso Web;

12.5.4. Ser capaz de verificar solicitações Web (HTTP e HTTPS), permitindo ou negando acessos baseados em regras definidas pelo CONTRATANTE;

12.5.5. Implementar mecanismos para categorizar novos sites da Web;

12.5.6. Implementar filtro de conteúdo Web com categorias de classificação de URLs e configuração de controle de acesso a estas categorias a serem consultadas no analisador de URLs;

12.5.7. Capaz de operar em modo man-in-the-middle para conexões do tipo HTTPS para controle de acesso e bloqueio a categorias, e também implementar bloqueio através do common-name do certificado do site;

12.5.8. Implementar a identificação de usuários e grupos, para efeito de detalhamento de filtragem do acesso (liberações ou bloqueios), totalmente compatível com Microsoft Active Directory 2003, 2008 e 2012 e superiores, utilizando-se credenciais LDAP, RADIUS e endereço IP;

12.5.9. Implementar bloqueio de arquivos que consomem banda, como MP3, streaming (áudio e vídeo) e/ou arquivos que possam conter códigos maliciosos, como por exemplo .exe e .zip;

12.6. Sistema de Antivírus de Gateway (AntiMalware de Gateway)

12.6.1. A solução de Antivírus de Gateway deve funcionar integrada ao Sistema de Firewall de Nova Geração (NGFW);

12.6.2. Deve ser capaz de monitorar o tráfego de rede e possuir proteção contra malwares como vírus, trojans, spywares, phishings;

12.6.3. Possuir mecanismo de atualização automática;

12.6.4. Identificar e bloquear códigos maliciosos nos protocolos HTTP, SMTP e FTP;

12.6.5. Permitir definição da ação a ser tomada de acordo com o tipo de arquivo examinado;

12.6.6. Ser um produto de detecção e eliminação de códigos maliciosos que esteja sob contínua evolução;

12.6.7. A CONTRATADA deve agir de forma proativa, atualizando as listas de malwares conhecidos periodicamente, ou imediatamente, sempre que tiver conhecimento da liberação de novas vacinas para detecção de malware dispersados recentemente (12 horas) na Internet.

12.6.8. Possuir mecanismo de análise heurística de vírus, configurável pelo administrador;

12.6.9. Deve ser capaz de analisar arquivos compactados no mínimo nos seguintes formatos: ZIP, Microsoft CAB, RAR, BZIP2 e TAR;

12.7. CONTROLE DE APLICAÇÕES WEB 2.0

12.7.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB 2.0;

12.7.2. A solução deve ser capaz de identificar qualquer tipo de aplicação Web 2.0 de camada 7, independente de porta e protocolo;

12.7.3. Possuir um reconhecimento de pelo menos 1.500(hum mil e quinhentas) aplicações diferentes, incluindo categorização para tráfego relacionado a aplicações peer-to-peer, redes sociais, acesso remoto, update de software, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

12.7.4. Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, social widgets com controle granular para usuários ou grupos de usuários;

12.7.5. Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund);

12.7.6. Deve possibilitar não apenas o bloqueio das aplicações, mas também de portas e protocolos.

12.7.7. Reconhecer pelo menos as seguintes aplicações: Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Google+, Google Talk, Tinder, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex;

12.7.8. A solução deverá possibilitar a diferenciação e controle de partes das aplicações, como por exemplo: bloquear o Gtalk chat e permitir o acesso ao Gmail;

12.7.9. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta padrão ou não;

12.7.10. Solução deve ser capaz de criar regras com várias categorias.

12.7.11. Deve possibilitar a permissão ou bloqueio de aplicações por pelos menos os seguintes critérios:

12.7.11.1. Aplicação da Web;

12.7.11.2. Categorias;

12.7.11.3. Nível de risco;

12.7.11.4. IP/Range de IP's/Redes;

12.7.11.5. Usuários do AD/LDAP;

12.7.11.6. Grupos de usuários;

12.7.12. Limitar a banda (download/upload) usada por aplicações;

12.7.13. Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e gerência;

12.7.14. Devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory;

12.7.15. Deve suportar o controle de aplicações conhecidas e possibilitar a inclusão de aplicações desconhecidas localmente, ou, através de ticket direto com o fabricante.

12.7.16. Deve possibilitar a diferenciação e controle granular específico das aplicações, como por exemplo: Gmail, Gmail Enterprise, Gmail-Drive, Gmail-file-transfer, Gmail-file-transfer-download, Gmail-file-transfer-upload, Inbox-by-Gmail, Gmail-chat, Gmail-video-chat, Gmail-Voice-Chat, Gmail-Voice-Video-Chat, Gmail-call-phone, Viber, Viber-file-transfer, Viber-Voice-Call, Viber-Voice-message, WhatsApp-Messenger, WhatsApp-Messenger-file-transfer, WhatsApp-Messenger-Web, WhatsApp-Messenger-Voice-Call;

12.7.17. Deve permitir o bloqueio de aplicações Proxies (ex.: Ultrasurf, GPass, FreeGate, Hopster, Tor, HotSpot Shield, etc);

12.7.18. Deve possibilitar a integração da solução com base do Active Directory, Ldap, Radius ou base local para criação de políticas. Possibilitando a criação de regras utilizando:

12.7.18.1. Usuários;

12.7.18.2. Grupo de usuários;

12.7.18.3. Máquinas (estações de trabalho);

12.7.18.4. Endereço IP;
12.7.18.5. Endereço de Rede;
12.7.18.6. Combinação das opções acima;

12.7.19. A Solução deve ter um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem;

12.7.20. Deve possibilitar a customização por regra utilizando as seguintes ações de controle:
12.7.20.1. Permitir;
12.7.20.2. Bloquear;
12.7.20.3. Monitorar;
12.7.20.4. Informar o usuário;

12.7.21. A solução deverá possuir uma interface de fácil utilização para buscas de Aplicações;

12.7.22. A solução deve prover a opção de editar a notificação de bloqueio e redirecionar o usuário para a página de remediação;

12.8. Sistema de Firewall de Aplicação Web - WAF (WEB APPLIACTION FIREWALL)

12.8.1. WAF – Appliance Virtual

12.8.1.1. A solução deve suportar a configuração em cluster e trabalhar no modo ATIVO/ATIVO.

12.8.1.2. Cada WAF – que será disponibilizado no ambiente virtual da CONTRATADA – deverá ser capaz de operar após sua configuração (*tunning*), com no máximo 16gb de RAM e 8vCPUs.

12.8.1.3. Suportar, no mínimo, 10.000 requisições por segundo na camada de aplicação.

12.8.2. WAF – Appliance Físico

12.8.2.1. A solução deve suportar a configuração em cluster e trabalhar no modo ATIVO/ATIVO.

12.8.2.2. Cada *appliance* deve ser fornecido com, no mínimo, 2 (duas) interfaces Gigabit Ethernet.

12.8.2.3. Suportar, no mínimo, 85.000 requisições por segundo na camada de aplicação;

12.8.3. Principais Características do Sistema de Firewall de Aplicação Web - WAF

12.8.3.1. Atender ao especificado no item **12.1.2** e subitem(s), quanto aos certificados.

12.8.3.2. Esta solução não poderá ser ofertada agregada a solução de firewall NGFW.

12.8.3.3. Deve suportar no mínimo **15 (quinze) servidores** WEB ou 15 (quinze) endereços IPs;

12.8.3.4. Suportar throughput mínimo de **1 (um) Gbps**.

12.8.3.5. Deve ser capaz de identificar tráfego proveniente de fontes maliciosas e fraudulentas;

12.8.3.6. Deverá detectar e mitigar ataques DoS e DDoS em camada de aplicação;

12.8.3.7. Deve bloquear ataques de origem consideradas maliciosas ou botnets;

12.8.3.8. Deverá atuar diretamente na camada 7 (aplicação) do modelo OSI e ser capaz de interceptar todas as requisições do cliente e as respostas do servidor Web.

12.8.3.9. Deverá ser capaz de detectar e bloquear ataques em HTTP, HTTPS, SOAP, XML- RPC, Web Service, entre outros.

12.8.3.10. Deve possuir robustez adequada ao tráfego de dados do CONTRATANTE;

12.8.3.11. Deverá adotar o conceito de "assinaturas de ataques" com intuito de detectar ataques específicos e o conceito de "anomalia de comportamento" para detectar ataques através de tráfego anormal.

12.8.3.12. Deverá adotar o conceito de "Modo Positivo" de aprendizado automatizado, capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório e ainda se é somente-leitura), cookies, arquivos XML, ações SOAP, e elementos XML.

12.8.3.13. Deverá proteger contra ataques de "Crawling";

12.8.3.14. Todos os ataques detectados deverão ser registrados em banco de dados. Esses logs serão analisados pela equipe de especialistas em ataques Web, da CONTRATADA, para que possa ser tomada a melhor medida de prevenção.

12.8.3.15. Ao detectar tentativas de ataques, a CONTRATADA deverá adotar, de imediato, as medidas de combate ao ataque identificado. No caso dessas medidas implicarem em interrupções e/ou descaracterização dos serviços em uso, a CONTRATADA deverá entrar em contato com o CONTRATANTE em no máximo, 2 (duas) horas, para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las.

12.8.3.16. O firewall de aplicação - WAF deverá trabalhar com certificados digitais permitindo autenticação criptográfica mútua entre servidor e usuário;

12.8.3.17. Possuir robustez contra ataques por tentativa de senhas (força bruta);

12.8.3.18. Possibilitar o bloqueio de ataques de origem consideradas maliciosas ou botnets;

12.8.3.19. Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários;

12.8.3.20. Deverá detectar e proteger contra as seguintes classes de ataques:

12.8.3.20.1. Violações do protocolo HTTP;
12.8.3.20.2. SQL Injection;
12.8.3.20.3. LDAP Injection;
12.8.3.20.4. Cookie Tampering;
12.8.3.20.5. Cross-Site Scripting (XSS);
12.8.3.20.6. Buffer Overflow;
12.8.3.20.7. OS Command Execution;
12.8.3.20.8. Remote Code Inclusion;
12.8.3.20.9. Server Side Includes (SSI) Injection;
12.8.3.20.10. Full path disclosure;
12.8.3.20.11. Information Leak;
12.8.3.20.12. Scanners de vulnerabilidade Web e Crawlers;
12.8.3.20.13. Worms e Web Shell Backdoors;
12.8.3.20.14. Cookie poisoning;
12.8.3.20.15. HTTP Request Smuggling;
12.8.3.20.16. Ameaças Web AJAX/JSON;
12.8.3.20.17. Checagem de consistência de formulários;
12.8.3.20.18. Cross Site Request Forgery (CSRF);

12.8.3.21. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.

12.8.3.22. Deverá possuir proteção baseada em assinaturas para prover proteção contra ataques conhecidos.

12.8.3.23. Possuir firewall XML.

12.8.3.24. Proteção e prevenção contra ataques de dia zero.

12.8.3.25. O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation).

12.8.3.26. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral;

12.8.3.27. Implementar a segurança de web services.

12.8.3.28. Deverá possuir controle de fluxo por aplicação, permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma, qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas, deverá ser bloqueado como uma tentativa de acesso ilegal.

12.8.3.29. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

12.8.3.30. Deve suportar no mínimo 10 (dez) servidores web com aproximadamente 15 (quinze) aplicações web cada, com acessos internos e externos ao CONTRATANTE; Minimamente compreendendo os servidores de aplicação JBoss AS (4,6,7 e superiores), WildFly (8 e superiores) e IIS (6.0 e superiores) e, excetuando-se os casos para os quais existam solicitações específicas do CONTRATANTE, nenhum equipamento localizado na rede externa ou interna Deve conseguir ter acesso aos servidores Web. Este acesso sempre Deve ser feito através do Firewall de Aplicação para os protocolos HTTP e HTTPS.

12.8.3.31. A solução deve suportar autenticação LDAP, RADIUS e ser totalmente integrada com Microsoft Active Directory 2003, 2008 e 2012 e superiores.

12.9. Solução de Comunicação para Redes Wireless

12.9.1. Access Point Wireless

12.9.1.1. Gerenciamento de solução de comunicação para redes wireless que será responsável pelas seguintes funções: gerenciamento, administração e configuração centralizada de no mínimo 30 (trinta) access points wireless, funções de segurança para acesso e tráfego de dados, gerenciamento de RF (Rádio Frequência) e Prevenção de Intrusão (Wireless IDS).

12.9.1.2. Controlador de access point wireless ou access points em modo auto-gerenciado, capaz de administrar e configurar remotamente de maneira centralizada estes dispositivos, aplicando regras de segurança para as redes wireless e exibindo as seguintes informações:

12.9.1.2.1. Listagem de access point wireless.

12.9.1.2.2. Informações de configuração access point wireless.

12.9.1.2.3. Utilização da rede.

12.9.1.2.4. Listagem de clientes wireless.

12.9.1.2.5. Detalhes dos access point wireless não autorizados (rogues) detectados.

12.9.1.3. Caso seja fornecida a solução com access points em modo auto-gerenciado, deverá possuir as seguintes características:

12.9.1.3.1. Implementar funcionamento em modo auto-gerenciado, sem necessidade de controladora wireless para configuração de seus parâmetros de rede wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF. Deve obedecer a todas as características descritas mesmo neste modo de funcionamento.

12.9.1.3.2. Deve ser redundante dentro do cluster e não deve depender única e exclusivamente de um elemento do cluster, ou seja, em caso de falha de um ou mais pontos de acesso, a solução deve continuar funcionando, mesmo que somente com um único ponto de acesso.

12.9.1.3.3. Deve disponibilizar um firewall statefull interno à solução, com definição das políticas baseadas na identidade do usuário autenticado.

12.9.1.3.4. O ponto de acesso deve permitir a conversão de modo auto-gerenciado para modo gerenciado por controlador WLAN através de interface gráfica, em browser padrão (HTTPS), e permitir que todos os demais pontos de acesso pertencentes ao mesmo cluster, também seja convertidos automaticamente.

12.9.1.3.5. Deve disponibilizar na interface gráfica informações de usuários conectados, qualidade de sinal e trafego de dados na rede.

12.9.1.4. Devem ser fornecidos access points wireless que atendam no mínimo as seguintes características:

12.9.1.4.1. Deverá possuir e acompanhar componentes que permita sua fixação em teto e parede;

12.9.1.4.2. Deverá atender simultaneamente aos padrões 802.11 b/g/n/ac 2.4GHz e 5GHz;

12.9.1.4.3. Deverá operar para conexão a rede local com no mínimo uma interface GIGABIT Ethernet, com conector RJ-45 Fêmea;

12.9.1.4.4. Deverá permitir sua energização, pela interface de rede descrita no item anterior, no padrão IEEE 802.3at PoE;

12.9.1.4.5. Deverá possuir LEDs indicativos do estado de operação;

12.9.1.4.6. Deverá possuir no mínimo 6 (seis) antenas internas (no mínimo 3X3 MIMO) ao access points wireless, em conformidade com o padrão IEEE 802.11a/b/g/n/ac;

12.9.1.4.7. Deverá selecionar automaticamente o canal de transmissão;

12.9.1.4.8. Deverá possuir suporte a pelo menos 08 (oito) SSIDs;

12.9.1.4.9. Deverá permitir habilitar e desabilitar a divulgação do SSID;

12.9.1.4.10. Deverá implementar Fast Roaming ou funcionalidade similar de forma a garantir o roaming sem perda de conexão e com integridade de sessão, dando suporte a aplicações em tempo real;

12.9.1.4.11. Deverá ser implantado o protocolo de autenticação Radius para acesso wireless a rede coorporativa;

12.9.1.4.12. Deverá ter filtros de acesso à rede baseados em endereços MAC;

12.9.1.4.13. Deverá fornecer acesso a internet para a rede wireless visitante através de HotSpot;

12.9.1.4.14. Deverá suportar otimizações no portal de access point wireless (Hotspot) para atender as necessidades do CONTRATANTE;

12.9.1.4.15. Deverá suportar acesso wireless a celulares, tablets e outros.

12.9.1.4.16. Visando a redundância da solução de rede sem fio, os access points deverão fornecer acesso à rede independentemente do controlador, ou caso contrário, deverá ser ofertado um controlador redundante.

12.9.1.4.17. O equipamento deverá possuir registro de homologação na ANATEL;

12.9.2. SWITCH PoE

12.9.2.1. Permitir instalação em gabinete de 19" (dezenove polegadas) sem adaptações/kits.

12.9.2.2. LEDs de identificação de atividades de status do sistema, de cada porta e de alimentação.

12.9.2.3. Fonte de alimentação AC de 100/240 V, 60 Hz, com chaveamento automático.

12.9.2.4. Possuir altura de no máximo 1U.

12.9.2.5. Suportar operação normal em temperaturas de 5ºC até 40°C.

12.9.2.6. Possuir 24 portas GigabitEthernet 1000Base-T autosense e autonegóciavel com suporte a conectores RJ-45 de acordo com o padrão IEEE 802.3ab. As portas deverão ser compatíveis com Fast Ethernet 100BASE-TX no padrão IEEE 802.3u.

12.9.2.7. Possuir, no mínimo, 2 (duas) portas 10GE com suporte à inserção de transceivers do tipo SFP+ (compatíveis com padrão IEEE 802.3ae).

12.9.2.7.1. Deverão ser fornecidos 2 (dois) cabos e 4 (quatro) módulos para uplink a 10 (dez) Gbps. Desses módulos, 2 (dois) deverão ser compatíveis com o equipamento ofertado e 2 (dois) compatíveis com o Switch DELL N3048 (Switch core existente no Cofen).

12.9.2.8. Implementar Power Over Ethernet (PoE) de acordo com o padrão IEEE 802.3at em todas as portas ethernet 10/100/1000 simultaneamente.

12.9.2.9. Arquitetura de switch Stackable (pilha), permitindo o empilhamento de no mínimo 6 (seis) unidades por caminhos redundantes através de cabo do tipo closed-loop, e com desempenho mínimo de 10 (dez) Gbps full-duplex por porta de empilhamento, não podendo ser utilizados portas Ethernet e as portas de uplink para empilhamento.

12.9.2.9.1. Deverão ser fornecidos 1 (hum) cabo e 2 (dois) módulos para o empilhamento a 10 (dez) Gbps.

12.9.2.10. Deve ser possível adicionar novos switches na pilha através de forma automática, sem configuração prévia do novo switch adicionado.

12.9.2.11. A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha além de permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.

12.9.2.12. Possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface DB9 ou USB ou RJ-45.

12.9.2.13. Deverá ser fornecido cabo de console compatível com a porta de console do equipamento a partir de computador equipado com porta USB, bem como o cabo para permitir o empilhamento.

12.9.2.14. Capacidade de comutação de no mínimo 88 (oitenta e oito) Gbps non-blocking, ou seja, 44 (quarenta e quatro) Gbps entrando e saindo simultaneamente.

12.9.2.15. Capacidade de encaminhamento de pacotes de no mínimo 33 (trinta e três) Mpps non-blocking com pacotes de, no máximo 128 (cento e vinte e oito) bytes, incluso cabeçalhos ethernet, TCP/UDP e Ipv4/IPv6.

12.9.2.16. Capacidade de armazenamento de no mínimo 8.000 (oito mil) endereços MAC.

12.9.2.17. Implementar a configuração de no mínimo 4000 (quatro mil) Vlans Ids.

12.9.2.18. Implementar a configuração de no mínimo 255 (duzentos e cinquenta e cinco) VLANs ativas simultaneamente.

12.9.2.19. Implementar as seguintes funcionalidades/padrões:

12.9.2.20. Padrão IEEE 802.3x (Flow Control);

12.9.2.21. Padrão IEEE 802.1d (Spanning Tree);

12.9.2.22. Padrão IEEE 802.1w (Rapid Spanning Tree);

12.9.2.23. Padrão IEEE 802.1s (Multiple Spanning Tree);

12.9.2.24. Padrão IEEE 802.3ad (Link Aggregation);

12.9.2.25. Padrão IEEE 802.1p (CoS – Class of Service);

12.9.2.26. Padrão IEEE 802.1x (Network Access Control);

12.9.2.27. VLANs segundo o padrão IEEE 802.1q;

12.9.2.28. IGMPv1,IGMPv2 e IGMPv3 snooping;

12.9.2.29. DHCP snooping ou funcionalidade similar que permita o bloqueio de servidores DHCP não autorizados na rede;

12.9.2.30. Espelhamento do tráfego de entrada e saída de múltiplas portas do switch em uma única porta, inclusive entre portas de diferentes unidades de uma pilha;

12.9.2.31. Espelhamento do tráfego de entrada e saída de múltiplas VLANs do switch em uma única porta, inclusive entre portas de diferentes unidades de uma pilha;

12.9.2.32. Mecanismos que viabilizem a limitação e controle do broadcast;

12.9.2.33. Mecanismos de proteção contra Destination Lookup Failure;

12.9.2.34. Mecanismos de proteção contra arp spoofing;

12.9.2.35. Encaminhamento de Jumbo Frames com tamanho mínimo de 9000 bytes nas portas Gigabit Ethernet;

12.9.2.36. Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED;

12.9.2.37. Implementar reconhecimento de Telefones IP e provisioná-los na VLAN de voz automaticamente.

12.9.2.38. Implementar IPv6.

12.9.2.39. Implementar a configuração de endereços IPv6 para gerenciamento.

12.9.2.40. Implementar resolução de endereços IPv4 e IPv6 (via consultas DNS) para nomes (hostnames) atribuídos aos ativos de rede.

12.9.2.41. Implementar ICMPv6 com as seguintes funcionalidades: ICMP request, ICMP Reply e ICMP Neighbor Discovery Protocol (NDP).

12.9.2.42. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet e SNMP sobre Ipv6.

12.9.2.43. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.

12.9.2.44. Implementar roteamento estático para os protocolos IPv4 e Ipv6.

12.9.2.45. Implementar limitação de tráfego de entrada permitindo variar a taxa de limitação com granularidade de 1 (um) Mbps por porta.

12.9.2.46. Implementar pelo menos 8 (oito) filas de QoS em Hardware por porta 1GE .

12.9.2.47. Implementar funcionalidades de controle e limitação de tráfego por classe de serviço.

12.9.2.48. Implementar classificação e marcação de pacotes baseada em endereço de origem.

12.9.2.49. Implementar classificação e marcação de pacotes baseada em porta de origem.

12.9.2.50. Implementar classificação e marcação de pacotes baseada em endereço de destino.

12.9.2.51. Implementar classificação e marcação de pacotes baseada em porta de destino.

12.9.2.52. Implementar classificação e marcação de pacotes baseada em marcação DSCP.

12.9.2.53. Implementar classificação e marcação de pacotes baseada em marcação IP Precedence.

12.9.2.54. Implementar classificação e marcação de pacotes baseada em CoS (“Class of Service” – nível 2).

12.9.2.55. Implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).

12.9.2.56. Implementar controle de acesso por porta segundo o padrão IEEE 802.1x, com configuração dinâmica da VLAN do usuário autenticado.

12.9.2.57. Ao considerar o padrão 802.1x, implementar configuração automática de VLAN de quarentena para a porta de dispositivos/usuários não autenticados.”.

12.9.2.58. Caso o dispositivo a ser conectado não possua cliente IEEE 802.1x, o switch o posicionará em uma VLAN default.

12.9.2.59. Implementar autenticação ao menos 2 (dois) dispositivos 802.1x por porta, para suporte à autenticação de sistemas operacionais virtualizados.

12.9.2.60. Implementar autenticação de dispositivos baseado no endereço MAC, via servidor RADIUS ou TACACS.

12.9.2.61. Implementar limitação de endereços MAC por porta. Os endereços MAC podem ser aprendidos automaticamente ou configurados manualmente.

12.9.2.62. Implementar listas de controle de acesso (ACLs), ou funcionalidade similar, baseadas em endereços MAC de origem e destino, endereçosIP de origem e destino, portas TCP e UDP.

12.9.2.63. Implementar definição de grupos de usuários, com diferentes níveis de acesso, ou possuir no mínimo 3 grupos de usuários pré-configurado.

12.9.2.64. Implementar controle de comandos para usuários ou grupos de usuários no equipamento

12.9.2.65. Implementar e suportar TACACS+ ou similar. O similar deve funcionar minimamente sobre TCP e ainda tratar os processos de Autenticação e autorização em separado.

12.9.2.66. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.

12.9.2.67. Implementar Private VLAN ou funcionalidade similar que permita segmentar uma VLAN em sub-domínios: uma VLAN primária e múltiplas VLANs secundárias.

12.9.2.68. Implementar gerenciamento da pilha de switches através de um único endereço IP.

12.9.2.69. Implementar os seguintes protocolos e funcionalidades de gerenciamento:

12.9.2.69.1. Secure Shell (SSHv2);

12.9.2.69.2. SNMPv2c e SNMPv3, com autenticação e criptografia;

12.9.2.69.3. CLI (Command Line Interface);

12.9.2.69.4. Syslog;

12.9.2.69.5. Gerenciamento por meio de interface gráfica (web browser) pelo protocolo HTTPS;

12.9.2.69.6. FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol) ou SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol);

12.9.2.69.7. NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);

12.9.2.70. Implementar capacidade de monitoração via comando de operação SNMP de, no mínimo:

12.9.2.70.1. de tráfego de interfaces;

12.9.2.70.2. de uso de CPU do processador;

12.9.2.70.3. de uso de memória do processador;

12.9.2.71. Implementar a MIB II - RFC 1213.

12.9.2.72. Implementar múltiplas imagens de firmware ou permitir a atualização da imagem por intermédio de download de servidor de rede.

12.9.2.73. Implementar versão do sistema operacional/firmware mais recente, ou seja, o equipamento deverá possuir a versão mais atual do sistema operacional na data da autorização do fornecimento.

12.9.2.74. Implementar o download e o upload de configurações.

12.9.3. PATCH PANEL

12.9.3.1. Deve possuir com 24 portas CAT6, compatível com conectores modulares de 8 vias do tipo RJ45, padrão IDC 110 para cabos na parte traseira;

12.9.3.2. Deve suportar a IEEE 802.3, 1000 BASE T, 1000 BASE TX, EIA/TIA-854, ANSI-EIA/TIA-862, ATM, Vídeo, Sistemas de Automação Predial, 10G-BASE-T (TSB-155) todos os protocolos LAN anteriores;

12.9.3.3. Deve atender às pinagens T568A e T568B;

12.9.3.4. Deve ser fornecido com guia traseiro para facilitar o roteamento dos cabos, bem como porta etiquetas com proteção transparante e etiquetas para identificação;

12.9.3.5. Deve possuir altura de 1U;

12.9.3.6. Deve possuir 19" de largura, conforme requisitos da norma ANSI/TIA-EIA-310E;

12.9.3.7. Deve ser fornecido com parafusos e arruelas para fixação e ainda com os conectores fêmea UTP;

12.9.3.8. Deve oferecer garantia de ZERO BIT ERROR em Fast e Gigabit Ethernet;

12.9.3.9. Deve atender à Diretiva Européia RoHS Compliant.

12.10. Centro de Operações de Segurança – SOC (Security Operation Center)

12.10.1. A CONTRATADA deverá monitorar, gerenciar e administrar remotamente equipamentos e softwares componentes das soluções fornecidas neste Edital e realizar a resposta a incidentes de segurança na rede do CONTRATANTE, 24 horas por dia, 7 dias da semana.

12.10.2. Manter 1 (um) Centro de Operações de Segurança (Security Operation Center - SOC) fora das dependências do CONTRATANTE administrando os sistemas de detecção a partir de um console centralizado, monitorando de forma proativa o tráfego "ENTRANTE" e "SAINTE" e as tentativas de intrusão, buscando e interrompendo ataques e atividades suspeitas em tempo real, 24 horas por dia, 7 dias da semana;

12.10.3. Envidar seus melhores esforços para que quaisquer ataques, invasões ou incidentes sofridos pelo CONTRATANTE em suas redes e/ou sistemas, sejam identificados, controlados, interrompidos ou cessados, em caráter provisório ou definitivo, mantendo o CONTRATANTE sempre a par de tais ocorrências;

12.10.4. Realizar pericia forense quando ataques a redes e/ou sistemas do CONTRATANTE sejam bem sucedidos, identificando em relatório próprio a vulnerabilidade explorada e o dano sofrido pelos sistemas. A CONTRATADA deverá propor soluções em caráter provisório ou definitivo indicando o responsável pela mesma;

12.10.5. Adotar, de imediato, as medidas de combate ao detectar tentativas de ataques. No caso dessas medidas implicarem em interrupções e/ou descaracterização dos serviços em uso, a empresa deverá entrar em contato com o CONTRATANTE em no máximo, 15 (quinze) minutos, para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las;

12.10.6. Monitorar o ambiente do CONTRATANTE utilizando canais de dados WAN próprios e dedicado a este fim, conectando a "solução de segurança" ao Centro de Operações de Segurança – SOC ("Rede de Gerência" e "Rede de Monitoração") da CONTRATADA com acesso restrito e por meio de conexão segura e criptografada;

12.10.7. Responsável por monitorar, gerenciar e administrar remotamente equipamentos e softwares componentes da solução fornecida neste Edital e realizar a resposta a incidentes de segurança na rede do CONTRATANTE, 24 horas por dia os 7 dias da semana.

12.10.8. Definir e implantar as rotinas de backup de todos os equipamentos componentes da solução de segurança. Nesse sentido, será responsabilidade da CONTRATADA o backup realizado pela própria;

12.10.9. Executar a gestão estratégica de cada equipamento ou software utilizado na solução de segurança, monitorando a utilização de CPU, memória e demais recursos monitoráveis, de forma a construir baselines com informações de, pelo menos, 3 (três) meses;

12.10.10. Executar procedimentos, resolver problemas e esclarecer dúvidas relacionadas com instalação, configuração, atualização, funcionamento e uso dos equipamentos necessários ao funcionamento da solução de segurança;

12.10.11. Fazer o ajuste fino (tunning) e às customizações de configuração de toda a solução, adequando-a ao ambiente da CONTRATANTE;

12.10.12. Informar sobre incidentes ou resultado de monitoração nos ativos sob gestão exclusiva do CONTRATANTE;

12.10.13. Monitorar e resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos equipamentos componentes da solução de segurança;

12.10.14. Monitorar o funcionamento de toda a solução deste Edital, 24 horas por dia, 7 dias da semana. Em caso de paralisação de equipamentos ou serviços monitorados, a equipe de especialistas da CONTRATADA deverá entrar em contato imediato com os responsáveis técnicos do CONTRATANTE informando o tipo de alerta e a solução do mesmo;

12.10.15. Realizar a manutenção da infraestrutura de segurança, atualizando patches, correções e versões ou releases mais recentes dos softwares;

12.10.16. Realizar a manutenção periódica de configurações, regras e políticas do ambiente monitorado remotamente ou on-site;

12.10.17. A data e a hora para execução dos procedimentos serão acordados com o CONTRATANTE, devendo ser executados prioritariamente fora dos horários de uso intenso da rede, no caso das sondagens interferirem no funcionamento normal dos equipamentos e/ou sistemas avaliados;

12.10.18. Para cada vulnerabilidade ou inconformidade apontada nos relatórios, a CONTRATADA deverá descrever a falha encontrada, indicar a(s) possível(eis) solução(ões) e o(s) responsável(eis) pela sua implantação. No caso de ainda inexistir uma solução específica, a CONTRATADA deverá indicar qual ação deverá ser tomada para que, de forma paliativa, o problema seja contornado até que esteja disponível uma solução definitiva (inclusive instruções para aplicação de correções em produtos de terceiros);

12.10.19. Caberá ao CONTRATANTE decidir pela implementação, ou não, de qualquer sugestão apresentada nos relatórios, assumindo a responsabilidade por problemas, que porventura vierem a ser causados nos equipamentos e serviços da rede, em função de ter optado por não acatar determinada recomendação;

12.10.20. O Centro de Operações de Rede da CONTRATADA deverá possuir, no mínimo, a seguinte infraestrutura:

12.10.20.1. Utilizar sistema de gerenciamento de CFTV, que viabilize o rastreamento de pessoas dentro do ambiente da CONTRATADA e cujas imagens possam ser recuperadas com no mínimo 30 (trinta) dias passados.

12.10.20.2. Possuir solução de monitoramento de disponibilidade e desempenho.

12.10.20.3. Possuir registro de entrada e saída de pessoas mantidos por pelo menos 30 (trinta) dias.

12.10.20.4. Efetuar registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao SOC;

12.10.20.5. O perímetro do SOC deve ser equipado com sensor de intrusão e alarmes contra acesso indevido;

12.10.20.6. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia.

12.10.20.7. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do contrato.

12.10.20.8. Ser configurado de forma que a falha de um dos equipamentos isoladamente não interrompa a prestação dos serviços.

12.10.20.9. Ter sistema de provimento ininterrupto de energia elétrica.

12.10.20.10. Ter componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes.

12.10.20.11. Caso os serviços de gerenciamento e monitoramento não sejam feitos no mesmo espaço físico que o SOC, todos os requisitos devem ser atendidos em todos os locais de prestação desses serviços;

12.11. Sistema de Segurança de Endpoint

12.11.1. Principais características:

12.11.1.1. Antimalware para estações de trabalho

12.11.1.2. Antimalware para servidores

12.11.1.3. Antimalware para ambientes virtualizados

12.11.1.4. Controles de aplicativos

12.11.1.5. Controles de dispositivos

12.11.1.6. Controles de Endpoint

12.11.1.7. Anti-APT

12.11.1.8. Gerenciamento unificado e centralizado de todas as funções

12.11.1.9. Detecção de comprometimento: vírus, malware, backdoors, hosts em comunicação com sistemas infectados por botnet, serviços da web vinculados a conteúdo malicioso.

12.11.2. Atender ao especificado no item **12.1.2** e subitem(s), quanto aos certificados.

12.11.3. Toda solução proposta deverá possuir funcionalidades integradas e administradas através de console de gerenciamento.

12.11.4. Segurança para servidores e estações de trabalho (antivírus, antispyware, IPS, anti-APT e firewall).

12.11.5. Suporte total aos sistemas operacionais cliente baseados minimamente nas plataformas: Mac OS, Windows 7, 8, 10 em todas as suas versões e nas arquiteturas 32 bits e 64 bits.

12.11.6. Suporte total aos sistemas operacionais servidor baseados nas plataformas: Windows Server 2003, 2008 e 2012 em todas as suas versões e nas arquiteturas 32 bits e 64 bits, tanto físicos como virtuais.

12.11.7. Atualizações automáticas das listas de definições de malware a partir de local predefinido da rede, ou de site da Internet.

12.11.8. Deve permitir atualização das definições de malware.

12.11.9. Frequência de atualização no mínimo diária e com possibilidade de agendamento.

12.11.10. Varredura em tempo real: de arquivos (gravação, renomeio e leitura), de processos em memória.

12.11.11. Detecção e remoção de programas maliciosos como spyware, adware, trojans, dialers, rootkits, etc.

12.11.12. Monitoramento em tempo real para a captura de malwares que são executados em memória sem a necessidade de escrever o arquivo.

12.11.13. Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise heurística.

12.11.14. Solução única para proteção contra malwares em geral, incluindo vírus, trojans, adware, rootkits, spywares, aplicações potencialmente indesejadas (PUAs), e buffer overflow.

12.11.15. Permitir bloqueio de portas.

12.11.16. Permitir criação de regras baseadas em processos de sistema.

12.11.17. Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia.

12.11.18. Oferecer proteção avançada de sistemas contra ameaças, tais como ataques aos navegadores.

12.11.19. Possuir proteção contra vulnerabilidades desconhecidas, tais como estouro de buffer (buffer overflow) e ataques de dia zero (zero-day attacks).

12.11.20. Possuir algum método de desinstalação de antivírus e minimamente dos seguintes fabricantes: Eset, Kaspersky, McAfee, Sophos, Symantec, Trend Micro e F-Secure.

12.11.21. Possuir instalação "silenciosa" através de Policies do Active Directory, script de logon, etc.

12.11.22. Permitir atualização automática das estações de trabalho através da console de gerenciamento.

12.11.23. Suportar o gerenciamento de no mínimo 1.000 (mil) máquinas a partir de um único servidor.

12.11.24. Permitir o gerenciamento do servidor utilizando os protocolos TCP/IP.

12.11.25. Permitir o gerenciamento centralizado da instalação nos clientes a partir de um único servidor, com possibilidade de Sincronização com o Active Directory.

12.11.26. Permitir a alteração das configurações dos antivírus nos clientes de maneira remota e através de regras aplicáveis a uma máquina, um grupo de máquinas, etc.

12.11.27. Permitir a atualização incremental e através do uso de políticas da lista de definições de vírus nos clientes a partir de um único ponto da rede.

12.11.28. Permitir a criação de tarefas de atualização, verificação de vírus e upgrades de produto em intervalos de tempo pré-determinados.

12.11.29. Permitir o armazenamento das informações coletadas nos clientes em um banco de dados SQL Server centralizado ou banco de dados proprietário.

12.11.30. Permitir diferentes níveis de administração da console de gerenciamento utilizando usuários do domínio.

12.11.31. Permitir forçar a configuração determinada no servidor para os clientes.

12.11.32. Caso o cliente altere a configuração da estação, a console deverá gerar um alerta em tempo real com possibilidade de envio de e-mail informando a atividade.

12.11.33. Exportação dos relatórios para pelo menos 2 (dois) dos seguintes formatos: PDF, XML, HTML, CSV, XLS, DOC e RTF.

12.11.34. Deve possuir Dashboard que forneça visibilidade em tempo real de incidência de malware, status de atualização das máquinas, bem como quaisquer avisos ou erros que possam ocorrer.

12.11.35. A solução deverá possui um Dashboard que contenha as seguintes informações:

12.11.35.1. Máquinas com a lista de definições de malware desatualizada.

12.11.35.2. Versão da solução de segurança instalada em cada máquina.

12.11.35.3. Os malwares que foram detectados.

12.11.35.4. Última comunicação com a console.

12.11.35.5. Data da última varredura (scan) completa.

12.11.36. Deve possuir a capacidade de geração de relatórios gráficos.

12.11.37. O controle de dispositivos deve ocorrer no mínimo para os seguintes dispositivos:

12.11.37.1. Drive de CD/DVD/Blue-Ray;

12.11.37.2. Dispositivos de armazenamento em massa (ex.: pen drives, memory cards, discos rígidos externos, etc.);

12.11.37.3. Dispositivos de certificação digital (Token e Smart Card);

12.11.37.4. Modem;

12.11.37.5. Dispositivos Wireless;

12.11.38. A solução deverá prover controle de dispositivos com no mínimo as seguintes características: Somente Leitura (Read only), Acesso Completo (Full Access) e Bloqueado (Blocked).

12.11.39. Deve permitir que o administrador defina uma White-List de dispositivos permitidos como Somente Leitura ou Acesso Completo.

12.11.40. Solução de controle de aplicativos para estações e servidores deverá ter as minimamente as seguintes características:

12.11.40.1. Verificação na execução;

12.11.40.2. Bloqueio da aplicação por seu nome de processo;

12.11.41. Deve permitir bloqueio de navegação em determinados sites com as seguintes características:

12.11.41.1. Lista de categorias específicas conforme o contexto, atualizadas automaticamente pelo fabricante;

12.11.41.2. Opção de adicionar sites em uma lista de liberação de sites que não devem ser bloqueados (white-list);

12.11.41.3. Opção de adicionar sites em uma lista de bloqueio de sites que devem ser bloqueados (black-list);

12.11.42. Capacidade de verificar a reputação de arquivos.

12.11.43. Deve possuir um controle de modificação do cliente Endpoint e contra a remoção não autorizada pelo cliente, possuindo uma senha.

12.11.44. Possibilitar a Instalação Remota.

12.11.45. Deve possibilitar a colocação dos equipamentos em quarentena, restringindo o acesso à rede para aqueles computadores que não estiverem em conformidade com as políticas, para no mínimo as seguintes premissas:

12.11.45.1. Computador deve possuir antivírus, atualizados e ativo;

12.11.45.2. Computador deve possuir firewall ativo;

12.11.45.3. Computador deve possuir antispyware, atualizado e ativo;

12.11.45.4. Computador deve possuir patches instalados, ativos e atualizados;

12.11.46. Possibilidade de recuperar arquivos da quarentena.

12.11.47. A solução deve possuir cache local na reputação de arquivos, possibilitando não varrer arquivos categorizados como não maliciosos e já escaneados anteriormente;

12.11.48. Possibilidade de recuperar instalação em clientes em caso de falha.

12.11.49. Deve ter a capacidade de iniciar à auto-remediação do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;

12.11.50. Deve ter a possibilidade de notificação customizada para o usuário.

12.12. Sistema de Gestão Contínua de Vulnerabilidades

12.12.1. Principais características:

12.12.1.1. Identificar novos ativos e novas portas em tempo real.

12.12.1.2. Verificar vulnerabilidades nos computadores servidores (Ex: protocolos inseguros, versões de serviços desatualizados, e outros).

12.12.1.3. Verificar vulnerabilidades nos dispositivos clientes (Ex: navegador desatualizado, softwares vulneráveis).

12.12.1.4. Escaneamento de vulnerabilidade para, minimamente: Dispositivos em rede, Hosts virtuais, Sistemas operacionais, Bancos de dados, Aplicativos web.

12.12.1.5. Deverá realizar o escaneamento para, no mínimo, 1.000 (hum mil) endereços IPs

12.12.2. Deverá ser capaz de detectar e avaliar vulnerabilidades encontradas nos sistemas e recursos de TIC do CONTRATANTE e na solução de segurança fornecida, especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas por meio de análises periódicas de conformidade.

12.12.3. Para efeito de comprovar a conformidade do ambiente implantado, a cada 90 (noventa) dias a CONTRATADA deverá realizar varreduras nos roteadores e equipamentos, que compõem o sistema, identificando e relatando possíveis vulnerabilidades encontradas;

12.12.4. Deverá verificar vulnerabilidades no ambiente para, no mínimo: detecção de hot fixes, service packs, registros, backdoors, trojans, malwares, peer to peer, portas de serviços habilitadas e antivírus;

12.12.5. Deverá detectar vulnerabilidades em aplicações baseadas em WEB, sistemas gerenciadores de banco de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede.

12.12.6. Deverá propor a aplicação de melhorias na topologia utilizada pelo CONTRATANTE.

12.12.7. Deverá sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades no ambiente de redes.

12.12.8. Deverá disponibilizar relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição dos ativos aos riscos identificados com, pelo menos, as seguintes informações: Descrição da vulnerabilidade, Plataforma (sistema operacional, servidor web, banco de dados, etc) e nível do risco.

12.12.9. Possuir relatórios que indiquem níveis de severidade para os problemas encontrados, de modo a priorizar as ações a serem desenvolvidas.

12.12.10. Os relatórios produzidos deverão ser submetidos à apreciação do CONTRATANTE, de modo que possa ser comprovada a conformidade do ambiente em produção e/ou aprovada a implementação de medidas identificadas como necessárias para correção de problemas apontados.

12.12.11. A Solução deve possuir uma base com testes de vulnerabilidades.

12.12.12. A Solução deve possuir em sua base de vulnerabilidades para cada item cadastrado, no mínimo as seguintes informações: nome, descrição, nível de risco, score CVSS BASE, referência (CVE, CWE, OSVDB, BugTrac ou outra fonte), solução e link para o download da correção – se aplicável, contramedidas – se aplicável, informação e fonte de exploit.

12.12.13. A Solução deve ser multiusuário, com níveis de permissões distintas.

12.12.14. A Solução deve possuir suporte aos protocolos IPV4 e IPV6.

12.12.15. A Solução deve possuir suporte a detecção de vulnerabilidades do tipo “zero-day”.

12.12.16. A Solução deve ser capaz de criar tickets para tratamento de vulnerabilidades, e distribuir estes para os usuários da Solução.

12.12.17. A Solução deve ser capaz de encerrar automaticamente os tickets quando a correção da vulnerabilidade for detectada.

12.12.18. A Solução deve prover cálculo de risco das vulnerabilidades identificadas, utilizando variáveis que possam ser personalizadas pelo usuário da ferramenta;

12.12.19. A Solução deve emitir relatório do tipo detalhado, com possibilidade de seleção das informações que irão compor o mesmo.

12.13. Serviço de Teste de Intrusão/Penetração (Pentest)

12.13.1. A atividade de Teste de Intrusão/Penetração (Pentest) deve compreender Testes de Invasão Externos e Internos e tem como objetivo principal identificar, controlar e corrigir possíveis vulnerabilidades nos sistemas, processos e ativos de infraestrutura tecnológica do CONTRATANTE. Estes testes envolvem o uso de técnicas e ferramentas para tentar o acesso privilegiado aos ativos e informações do CONTRATANTE por meio de simulações controladas de ataques reais, o ambiente do CONTRATANTE será avaliado em sua totalidade em busca de vulnerabilidades que possam permitir a obtenção de acesso não-autorizado.

12.13.2. O Teste de Negação de Serviço (DoS) deve compreender a verificação da quantidade e do tipo de tráfego suportado pela infraestrutura do CONTRATANTE, apresentar os riscos e as soluções para minimizar o impacto de um ataque de indisponibilidade real.

12.13.3. A CONTRATADA deverá realizar 02 (dois) testes por ocorrência, no mínimo 01 (uma) vez para a identificação dos problemas por meio de simulações de invasão ilícita e não

autorizada a ativos e informações (Teste de Invasão) a serem executadas internamente (através da rede interna do CONTRATANTE) e externamente (através da Internet), com duração de até 20 (vinte) dias cada simulação. O segundo teste, após a correção das mesmas pelo CONTRATANTE para a certificação de que foram efetivamente corrigidas para cada problema apontado em até 90 dias.

12.13.4. A CONTRATADA deverá compreender, minimamente: Teste prático dos controles de segurança existentes e Conhecimento das vulnerabilidades existentes;

12.13.5. A CONTRATADA deverá elaborar "Relatório de Teste de Invasão" para cada teste realizado apresentando todas as informações sobre o mesmo, contemplando no mínimo: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; descrição das ações realizadas; vulnerabilidades encontradas; categorização e severidade das vulnerabilidades, possíveis problemas aplicáveis, recomendações e controles de segurança necessários para correção das vulnerabilidades; apresentação das evidências apuradas; fontes de pesquisa, referências e ferramentas utilizadas.

12.13.6. A CONTRATADA deverá elaborar o "Plano de Teste de Invasão", para cada teste que será realizado, contemplando as informações de planejamento do teste, tais como: objetivos, premissas e escopo do teste; metodologia de análise de vulnerabilidades; equipe envolvida; prazos do teste.

12.13.7. Deverão ser testados, minimamente, os seguintes quesitos, quando pertinentes:

12.13.7.1. Validação de acesso lógico
12.13.7.2. Segmentos de rede
12.13.7.3. VLANs
12.13.7.4. Burlar regras de firewall
12.13.7.5. Obtenção de informações
12.13.7.6. Enumeração de usuários
12.13.7.7. Sniffing
12.13.7.8. ARP Spoofing
12.13.7.9. Segurança dos dados
12.13.7.10. Canal de comunicação
12.13.7.11. Cifras fracas
12.13.7.12. Armazenamento inseguro
12.13.7.13. Descoberta de Senhas
12.13.7.14. Força bruta
12.13.7.15. Ataque off-line
12.13.7.16. Arquitetura da rede
12.13.7.17. Acesso remoto e VPN
12.13.7.18. Protocolos de comunicação

12.13.8. Para o diagnóstico de segurança de aplicação Web que tem por objetivo encontrar vulnerabilidades e falhas em uma aplicação existente por meio de análise dinâmica (caixa preta/cinza), com a mesma perspectiva de qualquer outro usuário/visitante da aplicação, com ou sem credenciais de acesso, devem ser realizados testes específicos em formulários, páginas e funcionalidades disponíveis, com o objetivo de identificar problemas de segurança, testando minimamente, quando pertinente:

12.13.8.1. Validação de entrada
12.13.8.2. Sql Injection
12.13.8.3. Cross-Site Scripting (XSS)
12.13.8.4. Autenticação
12.13.8.5. Acesso anônimo
12.13.8.6. Captcha
12.13.8.7. Autorização

12.13.8.8. Acesso privilegiado
12.13.8.9. Abuso de funcionalidade
12.13.8.10. Gerenciamento de configuração
12.13.8.11. Páginas padrão
12.13.8.12. Upload
12.13.8.13. Dados confidenciais
12.13.8.14. Criptografia inadequada
12.13.8.15. Armazenamento de senhas
12.13.8.16. Gerenciamento de sessão

12.13.9. A CONTRATADA deverá elaborar um relatório de auditoria com os testes realizados, vulnerabilidades encontradas e recomendações de melhoria. O relatório técnico deve ser detalhado e deve ser acompanhado de uma apresentação executiva sobre os testes executados e seus resultados, assim como recomendações de medidas de correção e deve possibilitar à CONTRATANTE conhecer suas fragilidades e permitir criar os controles de segurança necessários para minimizar o risco de invasão.

12.13.10. A CONTRATADA deverá minimamente compreender atividades que busquem encontrar vulnerabilidades em potencial, de eventual má configuração, de falhas em hardwares e softwares desconhecidos, de técnicas de contra medidas ou deficiências no sistema;

12.13.11. A CONTRATADA deverá minimamente tentar a evasão de regras do firewall, acesso a roteadores, bancos de dados, sistemas operacionais e demais serviços de redes, captura de senhas, etc.

12.13.12. A CONTRATADA deverá realizar ataques de *man in the middle* (ARP Spoofing, captura de informações trafegando na rede) e tentativas de burlar firewall para a saída de informações.

12.13.13. A CONTRATADA deverá realizar ataques externos nos endereços de IP informados pelo CONTRATANTE, de forma a explorar possíveis vulnerabilidades nos serviços disponíveis.

12.13.14. A CONTRATADA deverá realizar dois tipos de teste de intrusão: tentativa de intrusão através do ambiente interno e tentativa de intrusão através do ambiente externo;

12.13.15. A CONTRATADA deverá testar servidores, estações e outros equipamentos da estrutura da rede com o objetivo de obter acesso a informações controladas.

12.13.16. A CONTRATADA deverá testar todos os roteadores e switches gerenciáveis do CONTRATANTE.

12.13.17. A CONTRATADA deverá verificar a existência de vulnerabilidades em access-points (redes sem fio) que possam ser acessadas externa ou internamente no CONTRATANTE.

12.13.18. O perfil mínimo dos profissionais deve ser compatível com o das atividades a serem desenvolvidas.

12.13.19. Os alvos dos "Testes de Invasão", bem como as premissas e condições para realização dos mesmos serão definidas e aprovadas pelo CONTRATANTE. Todas as fases dos "Testes de Invasão" poderão ser acompanhadas e supervisionadas a qualquer momento pelo CONTRATANTE. Quaisquer atividades com suspeita de comprometimento de algum ambiente ou ativo A CONTRATADA deverá ser imediatamente reportada ao CONTRATANTE, haja vista a necessidade de manter a disponibilidade dos ambientes, ativos e serviços do CONTRATANTE.

12.13.20. Os Testes deverão ser realizados, minimamente, por meio das seguintes abordagens: tentativa de intrusão na camada da rede e tentativa de intrusão na camada do aplicativo;

12.13.21. Os Testes de Intrusão poderão ser direcionados aos servidores Web e respectivas aplicações do serviço de hospedagem contratado pela CONTRATANTE.

13. SIGILO E INVIOLABILIDADE

13.1. A CONTRATADA compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

13.1.1. Política de segurança adotada pelo CONTRATANTE e configurações de hardware e software decorrentes;

13.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;

13.1.3. Processo de implantação no ambiente do CONTRATANTE, de mecanismos de criptografia e autenticação utilizados;

13.1.4. Recomendações e implementações decorrentes do processo de consultoria;

13.1.5. Quaisquer dados que a CONTRATADA venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do CONTRATANTE, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

13.1.6. Não fazer uso das informações prestadas pela CONTRATANTE que não seja em absoluto cumprimento ao contrato em questão.

13.1.7. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas.

13.1.8. A CONTRATADA obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

14. COMPROVAÇÃO DAS CARACTERÍSTICAS TÉCNICAS

14.1. O não atendimento às especificações técnicas descritas neste Termo de Referência implicará a desclassificação da proposta apresentada.

14.2. A comprovação do atendimento às características técnicas especificadas neste Termo de Referência dar-se-á por meio de catálogos, manuais e publicações originais e/ou apresentação de amostras.

14.3. A indicação do endereço eletrônico do catálogo do fabricante será aceita, como alternativa, para fins de averiguação das especificações dos produtos.

14.4. No conjunto de documentos apresentados pela licitante (folders/catálogos), para fins de aceitação, deverá vir indicando corretamente, a página, o documento e o trecho que comprove o atendimento de cada item/subitem da especificação técnica, conforme tabela abaixo.

Item/Especificação	Documento	Página	Comprovação

Tabela de comprovação dos itens técnicos

14.5. A proposta deverá apresentar com clareza a marca, o modelo, o tipo, a configuração e outras informações aplicáveis e necessárias à perfeita caracterização do dispositivo ou componente proposto, de forma a permitir a correta identificação deste na documentação técnica apresentada.

14.6. A proposta e a documentação técnica serão numeradas em ordem sequencial a partir da primeira página da proposta, devendo constar nesta o total de páginas.

14.7. As propostas serão analisadas por equipe de técnicos da CONTRATANTE no transcorrer do Pregão, para fins de verificação do atendimento às características da solução especificados neste Edital.

14.8. A análise técnica consistirá na verificação, por meio da documentação fornecida pela licitante ou obtida da Internet, do atendimento às especificações.

14.9. A falta de informações técnicas ou a incompatibilidade destas com as características especificadas implicará a desclassificação da proposta.

15. LOCAL DA REALIZAÇÃO DOS SERVIÇOS

15.1. Os serviços serão prestados no território do CONTRATANTE, presencialmente ou através de acesso remoto.

16. SUBCONTRATAÇÃO

16.1. Os serviços não poderão ser subcontratados no seu todo pela CONTRATADA, podendo, contudo, fazê-lo parcialmente, mantendo, porém, sua responsabilidade integral e direta perante o CONTRATANTE, mediante sua anuência expressa.

16.2. Em caso de subcontratação do objeto, esta deve efetivar-se, também, mediante contrato e somente após verificado o atendimento a todas as condições de habilitação constantes do edital e impostas às concorrentes que participaram do evento.

17. COMPLEMENTAÇÃO

17.1. O prazo de vigência do contrato será de 60 (sessenta) meses, contados a partir da assinatura do contrato, com eficácia após a publicação de seu extrato no Diário Oficial da União, com exceção dos itens com pagamento mensal/semestral, que terão vigência de 12 (doze) meses, renováveis até o limite permitido em lei.

17.2. Constituem-se em mandamentos e disposições gerais pertencentes a este termo de referência, os itens e subitens aqui descritos, possuindo todos a mesma importância, independentes ou não entre si, devendo ser observados e atendidos, não cabendo a nenhuma das partes reclamar o seu desconhecimento ou grau de relevância.

18. CONTEXTUALIZAÇÃO

18.1. O COFEN apresenta o seguinte cenário:

18.1.1. Utiliza de solução de antivírus gratuito, instalada, configurada e operante em seu parque tecnológico, contudo, a solução não possui o caráter proativo, fundamental para a detecção em tempo de real de códigos maliciosos e não possui o gerenciamento centralizado.

18.1.2. Utiliza de solução de Firewall que já foi descontinuada pelo fabricante e que não recebe mais atualizações, além de não suportar os novos paradigmas de segurança e tráfego criptografado em redes.

18.1.3. Recepciona um conjunto de colaboradores que trazem equipamentos particulares diversificados e sem autoridade do Departamento de Tecnologia da Informação e Comunicação como seus notebooks, tablets e smartphones pessoais com acesso à rede da instituição e trazendo potenciais vulnerabilidades.

18.1.4. Utiliza de uma rede sem fio corporativa que provê cobertura em todo edifício do COFEN por meio de antenas, meio passível de monitoração não autorizada e que é utilizado para trafegar dados corporativos.

18.1.5. Dispõe de uma biblioteca de livre acesso para o público da Enfermagem, o qual utiliza dos computadores ali disponíveis para fins de pesquisa e desenvolvimento de trabalhos.

18.1.6. Oferece um conjunto de serviços via Web cujos sistemas estão hospedados no datacenter do COFEN, disponibilizados pela Internet para outras instituições públicas e privadas e também para sociedade.

18.1.7. Comunica-se com os Conselhos Regionais para troca de informações críticas ao negócio do COFEN e do Sistema COFEN/Conselhos Regionais.

18.1.8. Está em constante reformulação e aperfeiçoamento de processos de negócios, incorporando tecnologias por meio de sistemas corporativos e ferramentas de apoio.

19. CARGA DE TRABALHO

19.1. O COFEN apresenta a seguinte carga:

Item	Volume/Quantidade	Descrição
Computadores Desktop	86	Windows 10
Computadores Desktop	90	Windows 7
Computadores Notebook/Ultrabook	50	Windows 7
Servidores Virtuais	40	Windows 2012
Servidores Físicos	6	Windows 2003
Hypervisor	WMWare VSphere 6	WMWare VSphere
Access Points	10	Wifi
Switches	15	LAN
Roteadores	2	LAN
Impressoras	16	LAN
Usuários fixos	200	
Caixas de e-mail	250	
Usuários móveis	100	
Servidores Web Internos	10	JBoss, Apache.
Aplicações WEB	36	Aplicações hospedadas no COFEN

20. ESTIMATIVA DE CONTRATAÇÃO

20.1. O COFEN estima adquirir **DURANTE** a vigência da Ata as seguintes quantidades para atendimento de necessidades atuais e futuras – que surgirão durante o seu prazo de validade (Quantitativos para montagem da Ata):

Lote	Descrição	Qtde Ofertada	Qtde Pretendida
1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A	1 Módulo (2 unidades)	1 Módulo
2	Sistema de Firewall de Nova Geração (NGFW) – TIPO B	1 Módulo (2 unidades)	0

3	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance FÍSICO	1 Módulo (2 unidades)	1 Módulo
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	1 Módulo (2 unidades)	1 Módulo
5	Sistema de Segurança para Endpoint – 50 licenças	1 Módulo (50 unidades)	8 Módulos
6	Solução de Comunicação para Redes Wireless - AP	1 unidade	30 unidades
7	Solução de Comunicação para Redes Wireless – Switch PoE	1 unidade	5 unidades
8	Solução de Comunicação para Redes Wireless – Patch Panel	1 unidade	5 unidades
9	Sistema de Gestão Contínua de Vulnerabilidades	1 unidade	1 unidades
10	Centro de Operações de Segurança – SOC (Security Operation Center)	1 unidade	1 unidade
11	Serviço de Teste de Intrusão/Penetração (Pentest)	2 unidades	1

20.2. O COREN - RJ estima adquirir **DURANTE** a vigência da Ata as seguintes quantidades para atendimento de necessidades atuais e futuras – que surgirão durante seu prazo de validade (Quantitativos para montagem da Ata):

Lote	**Descrição**	**Qtde Ofertada**	**Qtde Pretendida**
1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A (2 und)	1 Módulo (2 unidades)	1

2	Sistema de Firewall de Nova Geração (NGFW) – TIPO B	1 Módulo (2 unidades)	0
3	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance FÍSICO	1 Módulo (2 unidades)	0
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	1 Módulo (2 unidades)	1
5	Sistema de Segurança para Endpoint – 50 licenças	1 Módulo (50 unidades)	5
6	Solução de Comunicação para Redes Wireless - AP	1 unidade	25
7	Solução de Comunicação para Redes Wireless – Switch PoE	1 unidade	15
8	Solução de Comunicação para Redes Wireless – Patch Panel	1 unidade	6
9	Sistema de Gestão Contínua de Vulnerabilidades	1 unidade	1
10	Centro de Operações de Segurança – SOC (Security Operation Center)	1 unidade	1
11	Serviço de Teste de Intrusão/Penetração (Pentest)	2 unidades	1

20.3. O COREN - PI estima adquirir **DURANTE** a vigência da Ata as seguintes quantidades para atendimento de necessidades atuais e futuras – que surgirão durante seu prazo de validade (Quantitativos para montagem da Ata):

Lote	Descrição	Qtde Ofertada	Qtde Pretendida

1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A (2 und)	1 Módulo (2 unidades)	0
2	Sistema de Firewall de Nova Geração (NGFW) – TIPO B	1 Módulo (2 unidades)	1
3	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance FÍSICO	1 Módulo (2 unidades)	0
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	1 Módulo (2 unidades)	0
5	Sistema de Segurança para Endpoint – 50 licenças	1 Módulo (50 unidades)	1
6	Solução de Comunicação para Redes Wireless - AP	1 unidade	5
7	Solução de Comunicação para Redes Wireless – Switch PoE	1 unidade	1
8	Solução de Comunicação para Redes Wireless – Patch Panel	1 unidade	0
9	Sistema de Gestão Contínua de Vulnerabilidades	1 unidade	0
10	Centro de Operações de Segurança – SOC (Security Operation Center)	1 unidade	0
11	Serviço de Teste de Intrusão/Penetração (Pentest)	2 unidades	0

20.4. O COREN - PR estima adquirir **DURANTE** a vigência da Ata as seguintes quantidades para atendimento de necessidades atuais e futuras – que surgirão durante seu prazo de validade (Quantitativos para montagem da Ata):

Lote	Descrição	Qtde Ofertada	Qtde Pretendida
1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A (2 und)	1 Módulo (2 unidades)	1
2	Sistema de Firewall de Nova Geração (NGFW) – TIPO B	1 Módulo (2 unidades)	0
3	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance FÍSICO	1 Módulo (2 unidades)	1
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	1 Módulo (2 unidades)	0
5	Sistema de Segurança para Endpoint – 50 licenças	1 Módulo (50 unidades)	3
6	Solução de Comunicação para Redes Wireless - AP	1 unidade	4
7	Solução de Comunicação para Redes Wireless – Switch PoE	1 unidade	1
8	Solução de Comunicação para Redes Wireless – Patch Panel	1 unidade	0
9	Sistema de Gestão Contínua de Vulnerabilidades	1 unidade	0
10	Centro de Operações de Segurança – SOC (Security Operation Center)	1 unidade	0
11	Serviço de Teste de	2 unidades	0

	Intrusão/Penetração (Pentest)		

20.5. O COFEN estima adquirir **INICIALMENTE** as seguintes quantidades, para atendimento inicial das demandas existentes:

Lote	Descrição	Qtde Ofertada	Qtde Pretendida
1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A	1 Módulo (2 unidades)	1 Módulo
2	Sistema de Firewall de Nova Geração (NGFW) – TIPO B	1 Módulo (2 unidades)	0
3	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance FÍSICO	1 Módulo (2 unidades)	0
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	1 Módulo (2 unidades)	1 Módulo
5	Sistema de Segurança para Endpoint – 50 licenças	1 Módulo (50 unidades)	6 Módulos
6	Solução de Comunicação para Redes Wireless - AP	1 unidade	20 unidades
7	Solução de Comunicação para Redes Wireless – Switch PoE	1 unidade	2 unidades
8	Solução de Comunicação para Redes Wireless – Patch Panel	1 unidade	2 unidades
9	Sistema de Gestão Contínua de Vulnerabilidades	1 unidade	1 unidade
10	Centro de Operações de Segurança – SOC (Security Operation Center)	1 unidade	1 unidade

11	Serviço de Teste de Intrusão/Penetração (Pentest)	2 unidades	1

20.6. O CORENRJ estima adquirir **INICIALMENTE** as seguintes quantidades, para atendimento inicial das demandas existentes:

Lote	Descrição	Qtde Ofertada	Qtde Pretendida
1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A	1 Módulo (2 unidades)	1
2	Sistema de Firewall de Nova Geração (NGFW) – TIPO B	1 Módulo (2 unidades)	0
3	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance FÍSICO	1 Módulo (2 unidades)	0
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	1 Módulo (2 unidades)	0
5	Sistema de Segurança para Endpoint – 50 licenças	1 Módulo (50 unidades)	0
6	Solução de Comunicação para Redes Wireless - AP	1 unidade	10
7	Solução de Comunicação para Redes Wireless – Switch PoE	1 unidade	4
8	Solução de Comunicação para Redes Wireless – Patch Panel	1 unidade	4
9	Sistema de Gestão Contínua de Vulnerabilidades	1 unidade	1
10	Centro de Operações de	1 unidade	0

	Segurança – SOC (Security Operation Center)		
11	Serviço de Teste de Intrusão/Penetração (Pentest)	2 unidades	1

Cofen
Conselho Federal de Enfermagem

ANEXO I

Modelo da Proposta de Preços
(Pagamento sob demanda)

Lote	Descrição	Marca/ Modelo	Contra-tante		Qtde. TOTAL	Forma de Desembolso	Valor Unitário R$	Valor Total R$
1	Sistema de Firewall de Nova Geração (NGFW) – TIPO A (2 und)		DF	1 módulo (2 unidades)	3 módulos(6 unidades)	Único	296.036,05	888.108,16
			PR	1 módulo (2 unidades)				
			RJ	1 módulo (2 unidades)				
	Implantação da Solução		DF	1	3		12.346,67	37.040,00
			PR	1				
			RJ	1				
	Treinamento da Solução		DF	1	3		27.666,67	83.000,00
			PR	1				
			RJ	1				
	Workshop De Atualização		DF	4	12		9.902,64	118.831,68
			PR	4				
			RJ	4				
	Suporte Da Solução – Item 11.4		DF	1	3		22.726,67	68.180,00
			PR	1				
			RJ	1				
2	Sistema de Firewall de Nova Geração (NGFW) – TIPO B		PI	1 módulo (2 unidades)	1 módulo (2 unidades)	Único	110.198,07	110.198,07
	Implantação da Solução		PI	1	1		10.440,00	10.440,00
	Treinamento da Solução		PI	1	1		25.333,33	25.333,33
	Workshop de Atualização		PI	4	4		4.798,67	19.194,67
	Suporte da Solução – Item 11.4		PI	1	1		16.060,00	16.060,00
3	SISTEMA DE FIREWALL DE		DF	1 módulo (2 unidades)	2 módulos (4 unidades)	Único	809.396,56	1.618.793,12

	APLICAÇÃO WEB - WAF (WEB APPLICATION FIREWALL) APPLIANCE FÍSICO	PR	1 módulo (2 unidades)					
	Implantação da Solução	DF	1	2		101.773,33	203.546,67
		PR	1				
	Treinamento da Solução	DF	1	2		38.666,67	77.333,33
		PR	1				
	Workshop de Atualização	DF	4	8		9.465,33	75.722,67
		PR	4				
	Suporte da Solução – Item 11.4	DF	1	2		25.393,33	50.786,67
		PR	1				
4	Sistema de Firewall de Aplicação Web - WAF (Web Application Firewall) Appliance VIRTUAL	DF	1 módulo (2 unidades)	2 módulos (4 unidades)	Único	473.423,15	946.846,31
		RJ	1 módulo (2 unidades)				
	Implantação da Solução	DF	1	2		101.820,00	203.640,00
		RJ	1				
	Treinamento da Solução	DF	1	2		39.000,00	78.000,00
		RJ	1				
	WorkShop de atualização	DF	4	8		8.802,33	70.418,67
		RJ	4				
	Suporte da Solução – Item 11.4	DF	1	2		25.398,33	50.796,67
		RJ	1				
5	Sistema de Segurança para Endpoint – 50 licenças	DF	8 módulos (50 unidades)	17 módulos (850 unidades)	Único	11.567,50	196.647,50
		PI	1 módulo (50 unidades)				
		PR	3 módulos (50 unidades)				
		RJ	5 módulos (50 unidades)				
	Implantação da Solução	DF	1	4		10.153,33	40.613,33
		PI	1				
		PR	1				
		RJ	1				
	Treinamento da Solução	DF	1	4		22.666,67	90.666,67
		PI	1				
		PR	1				
		RJ	1				
	Suporte da Solução – Item 11.4	DF	1	4		14.395,00	57.580,00
		PI	1				
		PR	1				

		RJ	1				
6	Solução de Comunicação para Redes Wireless - AP	DF	30	64	Único	5.961,81	381.556,48
		PI	5				
		PR	4				
		RJ	25				
	Implantação da Solução	DF	1	4		12.440,00	49.760,00
		PI	1				
		PR	1				
		RJ	1				
	Treinamento da Solução	DF	1	4		19.333,33	77.333,33
		PI	1				
		PR	1				
		RJ	1				
	Suporte da Solução – Item 11.4	DF	1	4		13.396,67	53.586,67
		PI	1				
		PR	1				
		RJ	1				
7	Solução de Comunicação para Redes Wireless – Switch Poe	DF	5	22	Único	59.240,79	1.303.297,31
		PI	1				
		PR	1				
		RJ	15				
	Implantação da Solução	DF	1	4		21.773,33	87.093,33
		PI	1				
		PR	1				
		RJ	1				
	Treinamento da Solução	DF	1	4		22.000,00	88.000,00
		PI	1				
		PR	1				
		RJ	1				
	Suporte da Solução – Item 11.4	DF	1	4		16.730,00	66.920,00
		PI	1				
		PR	1				
		RJ	1				
8	SOLUÇÃO DE COMUNICAÇÃO PARA REDES WIRELESS – PATCH PANEL	DF	5	11	Único	4.975,00	54.725,00
		RJ	6				
	Instalação	DF	1	2		16.420,00	32.840,00
		RJ	1				
9	Sistema De Gestão Contínua de Vulnerabilidades	DF	1	2	Único	138.773,33	277.546,67
		RJ	1				
	Implantação da Solução	DF	1	2		22.440,00	44.880,00
		RJ	1				
	Treinamento da Solução	DF	1	2		22.666,67	45.333,33
		RJ	1				
	Suporte da Solução – Item 11.4	DF	1	2		36.730,00	73.460,00
		RJ	1				
TOTAL							**7.774.109,21**

OBS: NÃO SERÃO ACEITOS VALORES SUPERIORES AOS DESCRITOS .

Lote	Descrição	Contratante		Qtde. TOTAL	Forma de Desembolso	Valor Unitário R$	Valor Total 12 meses R$
10	CENTRO DE OPERAÇÕES DE SEGURANÇA – SOC (SECURITY OPERATION CENTER)	DF	1	2	Mensal	11.688,89	280.533,33
		RJ	1				
11	SERVIÇO DE TESTE DE INTRUSÃO/PENETRAÇÃO (PENTEST)	DF	2	4	Semestral	47.500,00	380.000,00
		RJ	2				
TOTAL							**660.533,33**

OBS: NÃO SERÃO ACEITOS VALORES SUPERIORES AOS DESCRITOS .

LOCAIS DE ENTREGA/INSTALAÇÃO

UF	ENTIDADE/ENDEREÇO
DF	Conselho Federal de Enfermagem – Cofen SCLN 304, Bloco E, Lote 9, Asa Norte, Brasília – CEP: 70.736-550
PI	Conselho Regional de Enfermagem do Piauí – Coren/PI Rua Magalhães Filho, nº 655 – Centro/Sul, Teresina – CEP: 64.001-350 e/ou subseções (http://www.coren-pi.com.br/)
PR	Conselho Regional de Enfermagem do Paraná – Coren/PR Rua XV de Novembro, nº 279 - 7º andar, Ed. Ascenção Fernandes – Centro, Curitiba – CEP: 80.020-921 e/ou subseções (https://www.corenpr.gov.br)
RJ	Conselho Regional de Enfermagem do Rio de Janeiro – Coren/RJ Av. Presidente Vargas, nº 502 - 9º andar – Centro, Rio de Janeiro – CEP: 20.071-000 e Rua da Glória, nº 190, Glória, Rio de Janeiro/RJ e/ou subseções (http://www.coren-rj.org.br)

Obs.: Os endereços das subseções poderão ser verificados nos sites dos respectivos Corens

ANEXO II DO EDITAL

MINUTA DE CONTRATO

CONTRATO ADMINISTRATIVO Nº. ____/2017

CONTRATO DE PRESTAÇAO DE SERVIÇOS, QUE ENTRE SI CELEBRAM O CONSELHO FEDERAL DE ENFERMAGEM – COFEN E A SOCIEDADE EMPRESÁRIA _____

CONTRATANTE: CONSELHO FEDERAL DE ENFERMAGEM – COFEN, entidade fiscalizadora do exercício profissional *ex* vi da Lei nº. 5.905, de 12/071973, com sede no SCLN 304, Bloco E, Lote 9, Asa Norte, Brasília/DF, CNPJ nº. 47.217.146/0001-57, representado, neste ato, por seu Presidente **Dr. MANOEL CARLOS NERI DA SILVA,** brasileiro, enfermeiro, portador da carteira COREN/RO nº. 63.592, inscrito no CPF sob o nº. 350.306.582-20, e por seu 1º Tesoureiro **Dr. JEBSON MEDEIROS DE SOUZA**, brasileiro, enfermeiro, portador da carteira profissional COREN/AC nº. 95621, inscrito no CPF sob o nº. 508.180.402-97.

CONTRATADA: _____, inscrita no CNPJ sob o nº _____, sediada na _____, neste ato representada pelo seu (cargo), Senhor (a) (inserir nome completo), portadora da Carteira de Identidade nº _____, expedida pela _____, e CPF nº _____, de acordo com a representação legal que lhe é outorgada por (procuração/contrato social/estatuto social).

Os CONTRATANTES têm entre si justo e avençado, e celebram o presente contrato, instruído no PAD nº 40/2015 (Pregão Eletrônico SRP - nº 17/2017), mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Aquisição por meio de **Sistema de Registro de Preços (SRP)**, de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o COFEN, compreendendo o fornecimento, a instalação, o suporte técnico, a garantia, o treinamento, o gerenciamento e o monitoramento de sistemas de: Firewall de Nova Geração (NGFW), Access Point Wireless, Switch PoE, Patch panel, Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web - WAF (Web Application Firewall), Centro de Operações de Segurança

da Informação - SOC (Security Operation Center), Teste de Intrusão/Penetração (Pentest), Endpoint, Gestão Contínua de Vulnerabilidades e assinaturas conforme especificações constantes no Termo de Referência (Anexo I do Edital do Pregão Eletrônico nº 17/2017).

CLÁUSULA SEGUNDA – DO PRAZO DE VIGÊNCIA

2.1. O prazo de vigência deste Termo de Contrato é aquele fixado no Edital, com início na data de ...../...../..... e encerramento em ...../...../....., podendo ser prorrogado por interesse das partes até o limite de 60 (sessenta) meses, desde que haja autorização formal da autoridade competente e observados os seguintes requisitos:

2.1.1. Os serviços tenham sido prestados regularmente;

2.1.2. A Administração mantenha interesse na realização do serviço;

2.1.3. O valor do contrato permaneça economicamente vantajoso para a Administração; e

2.1.4. A contratada manifeste expressamente interesse na prorrogação.

2.1.5. A CONTRATADA não tem direito subjetivo à prorrogação contratual.

2.2. A prorrogação de contrato deverá ser promovida mediante a celebração de termo aditivo.

CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DA CONTRATADA

3.1. Além das obrigações decorrentes da aplicação da Lei nº 10.520/02 subsidiariamente da Lei nº 8.666/93, do Decreto nº 5.450/2005, e demais normas pertinentes bem como, as especificações constantes do Anexo I do Termo de Referência do Edital de Pregão Eletrônico nº 17/2017, caberá à Contratada:

3.1.1. Responder, em relação aos seus funcionários, por todas as despesas decorrentes do fornecimento dos produtos e por outras correlatas, tais como salários, seguros de acidentes, tributos, indenizações, vales-refeição, vales-transporte e outras que porventura venham a ser criadas e exigidas pelo Poder Público;

3.1.2. Respeitar as normas e procedimentos de controle interno, inclusive de acesso às dependências do Conselho;

3.1.3. Responder pelos danos causados diretamente à Administração ou aos bens do Conselho, ou ainda a terceiros, decorrentes de sua culpa ou dolo, durante a execução do contrato, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo Conselho;

3.1.4. Efetuar a troca dos produtos ou manutenção dos serviços que não atenderem às especificações do objeto, no prazo assinado pelo Conselho;

3.1.5. Comunicar ao Conselho qualquer anormalidade constatada e manter, durante o período de vigência do Contrato, o atendimento das condições de habilitação exigidas neste Termo de Referência.

3.1.6. À Contratada caberá assumir a responsabilidade por:

3.1.6.1. Todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus empregados não manterão nenhum vínculo empregatício com o Conselho;

3.1.6.2. Todas as providências e obrigações estabelecidas na legislação específica de acidentes de trabalho, quando, em ocorrência da espécie, forem vítimas os seus empregados durante a execução do contrato, ainda que acontecido em dependência do Conselho;

3.1.6.3. Todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução do contrato, originariamente ou vinculada por prevenção, conexão ou continência;

3.1.6.4. Encargos fiscais e comerciais resultantes da contratação resultante deste Termo de Referência.

3.1.7. A inadimplência do licitante vencedor, com referência aos encargos sociais, comerciais e fiscais não transfere a responsabilidade por seu pagamento ao Conselho, nem poderá onerar o objeto desta contratação, razão pela qual o licitante vencedor renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o Conselho.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DO CONTRATANTE

4.1. Além das obrigações decorrentes da aplicação da Lei nº 10.520/02 subsidiariamente da Lei nº 8.666/93 e do Decreto nº 5.450/2005 e demais normas pertinentes bem como, especificações constantes do Anexo I do Termo de Referência do Edital de Pregão Eletrônico nº 17/2017, caberá ao Contratante:

4.1.1. Fornecer em tempo hábil, todos os elementos necessários para a prestação dos serviços;

4.1.2. Notificar imediatamente a Contratada sobre qualquer condição operacional anormal;

4.1.3. Efetuar o pagamento devido, segundo as condições estabelecidas;

4.1.4. Oferecer informações à Contratada, sempre que necessárias para execução dos trabalhos;

4.1.5. Aplicar as penalidades previstas no Edital da licitação, na hipótese da Contratada não cumprir com o compromisso assumido, mantidas as situações normais, arcando a empresa com quaisquer prejuízos que tal ato acarretar à Administração.

CLÁUSULA QUINTA – DA REMUNERAÇÃO E DA FORMA DE PAGAMENTO

5.1. O valor global deste Contrato é de **R$ _____** (.....), inclusos todos os custos e despesas, tais como e sem se limitar a: custos diretos e indiretos, tributos incidentes, lucros e outros necessários ao cumprimento integral do objeto deste Contrato.

5.2. O pagamento será realizado sob demanda executada, no mês subsequente a realização do serviço, de acordo com a quantidade atendida, após o cumprimento das etapas de implantação e efetiva utilização dos serviços, desde que todos os serviços estejam atestados pelo gestor;

5.3. O Cofen efetuará o pagamento, em moeda nacional corrente, por meio de Ordem Bancária, no prazo de 10 (dez) dias úteis, contados a partir da emissão do termo de aceite pelo gestor do contrato, juntamente com a entrega da Nota Fiscal/Fatura;

5.4. Ocorrendo a não aceitação pela fiscalização do Cofen dos serviços faturados, o fato será imediatamente comunicado à Contratada, para retificação das causas de seu indeferimento;

5.5. A nota fiscal deve estar preenchida com a descrição detalhada dos itens do objeto, o número do Contrato e os dados bancários da Contratada;

5.5.1. Junto com a Nota Fiscal, deverá apresentar a comprovação de regularidade, junto ao Sistema da Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (FGTS), às Fazendas Federal, Estadual e Municipal do domicílio ou sede da Contratada e da certidão negativa de débitos trabalhistas (CNDT), sem que isso gere direito a alteração de preços ou compensação financeira.

5.5.2. O não envio das certidões juntamente com as notas fiscais, ou ainda que as mesmas estejam disponíveis para emissão, não desobriga o Cofen de efetuar o pagamento das Notas Fiscais que constem serviços devidamente prestados e atestados pelo gestor do Contrato. Porém o desatendimento pela Contratada ao descrito pode motivar a rescisão contratual, a execução da garantia para ressarcimento dos valores e indenizações devidas à Administração e a aplicação das penalidades previstas no art. 87 da Lei nº 8.666/93.

5.6. Os pagamentos poderão ser descontinuados pelo Cofen, nos seguintes casos:

a) Não cumprimento das obrigações da Contratada para com terceiros, que possam, de qualquer forma, prejudicar o Cofen;

b) Inadimplemento de obrigações da Contratada para com o Cofen por conta do Contrato;

c) Erros ou vícios nas faturas.

5.7. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão

calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes formulas:

$$I = \frac{(TX/100)}{365}$$

EM = I x N x VP, onde:

I = Índice de atualização financeira;

TX = Percentual da taxa de juros de mora anual;

EM = Encargos moratórios;

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

VP = Valor da parcela em atraso.

5.8. Na hipótese de pagamento de juros de mora e demais encargos por atraso, os autos devem ser instruídos com as justificativas e motivos, e ser submetidos à apreciação da autoridade superior competente, que adotará as providências para verificar se é ou não caso de apuração de responsabilidade, identificação dos envolvidos e imputação de ônus a quem deu causa;
5.9. Não será efetuado nenhum pagamento antecipado, nem por serviços não executados.

CLAUSULA SEXTA – DA SUBCONTRATAÇÃO
6.1. Os serviços não poderão ser subcontratados no seu todo pela CONTRATADA, podendo, contudo, fazê-lo parcialmente, mantendo, porém, sua responsabilidade integral e direta perante o CONTRATANTE, mediante sua anuência expressa.
6.2. Em caso de subcontratação do objeto, esta deve efetivar-se, também, mediante contrato e somente após verificado o atendimento a todas as condições de habilitação constantes do edital e impostas às concorrentes que participaram do evento.

CLÁUSULA SÉTIMA – DA DOTAÇÃO ORÇAMENTÁRIA
7.1. As despesas decorrentes deste contrato correrão por conta do Código de Despesa de n°: .....

CLÁUSULA OITAVA – DAS PENALIDADES
8.1. Com fundamento no artigo 7º da Lei n.º 10.520/2002 e no art. 28 do Decreto n.º 5.450/2005, ficará impedida de licitar e contratar com a União, Estados, Distrito Federal e Municípios e será descredenciada do Sicaf e do cadastro de fornecedores da Contratante, pelo prazo de até 5 (cinco) anos, garantida a ampla defesa, sem prejuízo das demais cominações legais e de multa de até 30% (trinta por cento) sobre o valor da contratação, sem prejuízo da rescisão unilateral do contrato (art. 78 da Lei 8.666, de 1993), a Contratada que:

8.1.1. Não assinar o termo de contrato ou aceitar/retirar o instrumento equivalente, quando convocado dentro do prazo de validade da proposta;
8.1.2. Apresentar documentação falsa;
8.1.3. Deixar de entregar os documentos exigidos no certame;
8.1.4. Ensejar o retardamento da execução do objeto;
8.1.5. Não mantiver a proposta;
8.1.6. Cometer fraude fiscal;
8.1.7. Comportar-se de modo inidôneo;

8.2. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os licitantes, em qualquer momento da licitação, mesmo após o encerramento da fase de lances.
8.3. O licitante/adjudicatário que cometer qualquer das infrações discriminadas no subitem anterior ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

8.3.1. Multa de 5% (cinco por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do licitante;

8.3.2. Impedimento de licitar e de contratar com a União e descredenciamento no SICAF, pelo prazo de até cinco anos;

8.4. A penalidade de multa pode ser aplicada cumulativamente com a sanção de impedimento.

8.5. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao licitante/adjudicatário, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente na Lei nº 9.784, de 1999.

8.6. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

CLÁUSULA NONA – DA GARANTIA CONTRATUAL

9.1. A Contratada deverá apresentar no prazo máximo de 10 (dez) dias, contados da data de assinatura do instrumento contratual, garantia de 5% (cinco por cento) do valor contratual estimado para 12 (doze) meses, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, nos termos do Paragrafo 1º do artigo 56, da Lei nº 8.666/93;

9.2. A garantia assegurará qualquer que seja a modalidade escolhida, o pagamento de:

9.2.1 Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

9.2.2 Prejuízos causados ao Contratante ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

9.2.3 As multas moratórias e punitivas aplicadas pelo Contratante à Contratada;

9.2.4 Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela contratada;

9.3. A contratada se obriga a apresentar a garantia para o período integral da vigência contratual, e, no caso de prorrogação do contrato, mantê-la válida e atualizada;

9.4. A perda da garantia em favor do Contratante, por inadimplemento das obrigações contratuais, far-se-á de pleno direito, independente de qualquer procedimento judicial ou extrajudicial das demais sanções previstas no contrato;

9.5. A garantia deverá ser integralizada sempre que dela forem deduzidos quaisquer valores e nos casos de prorrogação de prazo ou acréscimo de valores deverá ser atualizada na mesma proporção em conformidade com o art. 56, § 2º da Lei 8.666/93;

9.6. A qualquer tempo poderá ser admitida a substituição da garantia, observadas as modalidades previstas no artigo 56 da Lei nº 8.666/93;

9.7. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do contrato por dia de atraso, até o máximo de 2% (dois por cento);

9.8. O atraso superior a 30 (trinta) dias autoriza o Contratante a promover a retenção dos pagamentos devidos à Contratada, até o limite de 5% (cinco por cento) do valor anual do contrato, a título de garantia, com correção monetária, em favor da contratada;

9.9. Será considerada extinta a garantia:

9.9.1 Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

9.9.2 Com a extinção do contrato.

9.10. A garantia sempre terá prazo de cobertura findando 03 (três) meses, após, o término da vigência contratual, conforme inciso XIX do art. 19 da Instrução Normativa nº 06, de 23 de dezembro de 2013.

9.11. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Contratante, com o objetivo de apurar prejuízos e/ou aplicar sanções à contratada.

CLÁUSULA DÉCIMA – DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO AO EDITAL E AO CONTRATO

10.1. O presente contrato fundamenta-se na Lei n.º 8.666/1993 e vincula - se ao Edital e anexos do Pregão Eletrônico nº 17/2017, bem como à proposta da CONTRATADA, constantes do PAD n.º 40/2015, independentemente de transcrição.

CLÁUSULA DECIMA PRIMEIRA - DO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

11.1. A fiscalização da execução do objeto do contrato será exercida por servidor nomeado pelo Contratante, nos termos do artigo 67 e 73 da Lei nº 8.666/93;

11.2. Ao Contratante reserva-se o direito de rejeitar, no todo ou em parte, os itens/serviços fornecidos em desacordo com o estabelecido no presente contrato;

11.3. A fiscalização exercida pelo Gestor do Contratante não excluirá ou reduzirá a responsabilidade da Contratada pela completa e perfeita execução dos itens deste contrato.

CLAÚSULA DÉCIMA SEGUNDA– DO REAJUSTE

12.1 A periodicidade de reajuste do valor do presente CONTRATO será anual, contada a partir da data-limite para a apresentação da proposta, conforme disposto na Lei nº 10.192 de 14/02/2001, utilizando-se a variação do IGP-DI da Fundação Getúlio Vargas, mediante aplicação do índice do mês anterior à data-limite da apresentação da proposta e do índice do mês anterior ao mês previsto para o reajustamento.

12.2 No cálculo do 1º reajuste deverá ser utilizado o índice do mês anterior à data da proposta comercial e o índice do mês anterior à data prevista para o reajuste.

12.3 Para os reajustes subsequentes será utilizado o índice do mês anterior à data de concessão do último reajuste do CONTRATO e o índice do mês anterior à data prevista para o reajuste.

12.4 À época devida, a CONTRATADA habilitar-se-á ao pagamento do reajuste com apresentação de Notas Fiscais/Fatura distintas:

a) Uma relativa ao valor mensal reajustado.
b)Outra referente ao valor retroativo, se houver.

CLAÚSULA DÉCIMA TERCEIRA – DA RESCISÃO

13.1. O presente Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 78 da Lei nº 8.666, de 1993, com as consequências indicadas no art. 80 da mesma Lei, sem prejuízo da aplicação das sanções previstas no Termo de Referência, anexo do Edital.

13.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

13.3. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 77 da Lei nº 8.666, de 1993.

13.4. O termo de rescisão, sempre que possível, será precedido:

12.4.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

12.4.2. Relação dos pagamentos já efetuados e ainda devidos;

12.4.3. Indenizações e multas.

CLÁUSULA DÉCIMA QUARTA – ALTERAÇÕES

14.1. Eventuais alterações contratuais reger-se-ão pela disciplina do art. 65 da Lei nº 8.666, de 1993.

14.2. A CONTRATADA é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

14.3. As supressões resultantes de acordo celebrado entre as partes contratantes poderão exceder o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

CLÁUSULA DÉCIMA QUINTA – PUBLICAÇÃO

15I.1. Incumbirá à CONTRATANTE providenciar a publicação deste instrumento, por extrato, no Diário Oficial da União, no prazo previsto no artigo 61, da Lei nº 8.666, de 1993.

CLÁUSULA DÉCIMA SEXTA – DO FORO

16.1. As partes elegem de comum acordo, a Justiça Federal, no Foro da cidade de Brasília/DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro, por mais privilegiado que seja, para a solução dos conflitos eventualmente decorrentes da presente relação contratual, nos termos do art. 55, § 2º, da Lei nº. 8.666, de 21 de junho de 1993.

E por estarem justos e contratados, lavram o presente instrumento de contrato em três vias de igual teor, que vão assinados pelas partes, que se comprometem a cumprir o presente em todas as suas cláusulas e condições.

Brasília, _____ de _____ de 2017.

_____ _____

CONTRATANTE
MANOEL CARLOS NERI DA SILVA
Presidente

CONTRATADA

_____

CONTRATANTE
JEBSON MEDEIROS DE SOUZA
1º Tesoureiro

_____

ALBERTO JORGE SANTIAGO CABRAL
Procurador Geral

TESTEMUNHAS:

_____ _____

ANEXO III DO EDITAL
MODELO DE PROPOSTA DE PREÇOS

PREGÃO ELETRÔNICO SRP - COFEN Nº: 17/2017
PROPOSTA DE PREÇOS

NOME DA EMPRESA:_____

DATA: _____

1. OBJETO

1.1. Aquisição por meio de **Sistema de Registro de Preços (SRP)**, de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o COFEN, compreendendo o fornecimento, a instalação, o suporte técnico, a garantia, o treinamento, o gerenciamento e o monitoramento de sistemas de: Firewall de Nova Geração (NGFW), Access Point Wireless, Switch PoE, Patch panel, Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web - WAF (Web Application Firewall), Centro de Operações de Segurança da Informação - SOC (Security Operation Center), Teste de Intrusão/Penetração (Pentest), Endpoint, Gestão Contínua de Vulnerabilidades e assinaturas conforme especificações constantes no Termo de Referência (Anexo I do Edital do Pregão Eletrônico nº 17/2017).

2. PLANILHA DE PREÇOS

2.1 Apresentar planilha descritiva com os valores unitários, conforme descrito no anexo I do termo de referencia.

OBS: Não serão aceitos valores superiores aos descritos na planilha, anexo I do termo de referência.

- Validade da Proposta: ___ (_____) dias, observado o prazo mínimo de sessenta (60) dias.
- Nos preços apresentados deverão incluir todos os custos com salários, horas extras, encargos sociais, transportes, uniformes, lucros, encargos fiscais e para-fiscais, despesas diretas e indiretas, bem como aquelas indispensáveis para execução dos serviços licitados.
- Declaramos que os produtos aqui ofertados estão de acordo com as especificações do termo de referencia.
- Declaramos conhecer e nos submetemos integralmente a todas cláusulas e condições do presente Edital.

VALOR TOTAL DA PROPOSTA: R$ _____ (_____)
VALIDADE DA PROPOSTA:

CNPJ:

ASSINATURA:

ANEXO IV DO EDITAL
MINUTA DA ATA DE REGISTRO DE PREÇOS
PREGÃO ELETRÔNICO SRP - COFEN Nº: 17/2017

Na data consignada abaixo o Conselho Federal de Enfermagem – COFEN, CONSELHO FEDERAL DE ENFERMAGEM – COFEN, entidade fiscalizadora do exercício profissional *ex* vi da Lei nº. 5.905, de 12/071973, com sede no SCLN 304, Bloco E, Lote 9, Asa Norte, Brasília/DF, CNPJ nº. 47.217.146/0001-57, representado, neste ato, por seu Presidente **Dr. MANOEL CARLOS NERI DA SILVA,** brasileiro, enfermeiro, portador da carteira COREN/RO nº. 63.592, inscrito no CPF sob o nº. 350.306.582-20, e por seu 1º Tesoureiro **Dr. JEBSON MEDEIROS DE SOUZA**, brasileiro, enfermeiro, portador da carteira profissional COREN/AC nº. 95621, inscrito no CPF sob o nº. 508.180.402-97, na qualidade de ÓRGÃO GERENCIADOR, de outro lado a empresa ..... com sede na ....., na cidade ....., Estado ....., inscrita no Cadastro Nacional da Pessoa Jurídica do Ministério da Fazenda sob o nº ....., neste ato representada por seu representante legal, , nome....., nacionalidade....., estado civil....., profissão....., identidade..... e CPF....., abaixo assinado, de conformidade com os poderes que lhe são conferidos e que constam do seu Contrato Social / Estatuto Social, acordam proceder, nos termos das Leis 8.666/93 e 10.520/02, do Decreto n° 7.892/13, com suas alterações posteriores, bem como do Edital de Pregão em epígrafe, ao REGISTRO DE PREÇOS dos itens descritos no Anexo I do termo de referencia, com seus respectivos preços unitários.

CONDIÇÕES GERAIS

1. DO OBJETO

1.1 A presente Ata de Registro de Preços tem por objeto aquisição por meio de **Sistema de Registro de Preços (SRP)**, de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o COFEN, compreendendo o fornecimento, a instalação, o suporte técnico, a garantia, o treinamento, o gerenciamento e o monitoramento de sistemas de: Firewall de Nova Geração (NGFW), Access Point Wireless, Switch PoE, Patch panel, Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web - WAF (Web Application Firewall), Centro de Operações de Segurança da Informação - SOC (Security Operation Center), Teste de Intrusão/Penetração (Pentest), Endpoint, Gestão Contínua de Vulnerabilidades e assinaturas

2. DA VALIDADE DO REGISTRO DE PREÇOS

2.1. A Ata de Registro de Preços terá efeito de compromisso de prestação de serviços, ficando o fornecedor nela incluído obrigado a celebrar as Ordens de Execução de Serviços (OS) ou Contratos, conforme o caso, que advierem, nas condições estabelecidas no Edital e em seus anexos e nesta Ata, cuja validade será de 12 (doze) meses, contados a partir da data de sua publicação no Diário Oficial.
2.2. Os valores registrados na Ata serão válidos por 12 (doze) meses, contados a partir da data de sua publicação no Diário Oficial.
2.2. A existência de preços registrados não obriga o COFEN ou a Empresa Participante do Registro de Preços a firmarem as contratações que deles poderão advir, ficando-lhes facultada a realização de licitação específica para a contratação do objeto de que trata esta Ata, sendo, contudo, assegurado ao(s) beneficiário(s) do Registro(s) de Preços, a preferência da prestação dos serviços em caso de igualdade de preços.

3. DOS VALORES REGISTRADOS

3.1. Os valores das verbas estimadas dos participantes deste registro de preços são:

ORGÃO	QTD	VLR UNITÁRIO	VLR TOTAL

4. DO CANCELAMENTO DO REGISTRO DE PREÇOS

4.1. O fornecedor terá seu registro cancelado quando:

a) Descumprir as condições da Ata de Registro de Preços;

b) Não assinar o Instrumento Contratual no prazo estabelecido pelo COFEN, sem justificativa aceitável, quando for o caso;

c) Não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

d) Sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da Lei 8.666, de 1993, ou no art. 7º da Lei 10.520, de 2002; ou

e) Por razões de interesse público, em virtude de fato superveniente, decorrente de caso fortuito ou força maior, que prejudique o cumprimento da ata, devidamente comprovados e justificados.

3.1.1. O cancelamento de registro, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do COFEN.

3.1.2. O fornecedor poderá solicitar o cancelamento do seu registro de preço na ocorrência de fato superveniente que venha comprometer a perfeita execução contratual, decorrentes de caso fortuito ou de força maior devidamente comprovados e justificados.

4. DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

4.1. O Conselho Federal de Enfermagem – Cofen será o Órgão Gerenciador, sendo, portanto, o responsável pela condução da licitação e gerenciamento da Ata de Registro de Preços.

4.2. Os Conselhos Regionais de Enfermagem – Coren's poderão ser Órgãos Participantes, conforme previsto no artigo 6º, do Decreto nº. 7892/2013, desde que façam a manifestação.

4.3. A Ata de Registro de Preços terá validade de 12 (doze) meses, contados a partir da data de sua assinatura, com eficácia após sua publicação no Diário Oficial.

4.4. A Ata de Registro de Preços terá efeito de compromisso de fornecimento, ficando os fornecedores nela incluídos obrigados a celebrar as ordens de fornecimento ou contratos que advierem nas condições estabelecidas neste edital.

4.5. A adesão ao registro de preços decorrente do presente edital, esta restrita aos Conselhos regionais de Enfermagem, os quais fazem parte do Sistema Cofen/Corens.

4.6. As aquisições ou contratações adicionais decorrentes da adesão à Ata de Registro de Preços não poderão exceder, por Conselho Regional, a cem por cento dos quantitativos dos itens registrados na Ata de Registro de Preços para o órgão gerenciador e órgãos participantes.

4.7. Homologado o resultado deste Pregão, a licitante mais bem classificada será convocada para assinar a Ata de Registro de Preços, no prazo de até 3 (tres) dias úteis, contado da data do recebimento do documento oficial de convocação.

4.7.1. O prazo para que a licitante mais bem classificada compareça após ser convocada, poderá ser prorrogado, uma única vez, por igual período, desde que ocorra motivo justificado e aceito pelo Conselho Federal de Enfermagem.

4.7.2. É facultado ao Conselho Federal de Enfermagem, quando a convocada não assinar a Ata de Registro de Preços no prazo e condições estabelecidos, convocar as licitantes

remanescentes, na ordem de classificação, para fazê-lo em igual prazo, nos termos do art. 4º, inciso XXIII, da Lei 10.520/02.

4.8. Publicada na Imprensa Oficial, a Ata de Registro de Preços implicará compromisso de fornecimento nas condições estabelecidas, conforme disposto no artigo 14 do Decreto n.º 7.892/2013.

4.9. A existência de preços registrados não obriga a Administração a contratar, facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

4.10. O prazo de validade improrrogável da Ata de Registro de Preços será de no máximo 12 (doze) meses, contado da data da sua assinatura, excluído o dia do começo e incluído o do vencimento.

4.11. Durante a vigência da Ata, os preços registrados serão fixos e irreajustáveis, exceto nas hipóteses decorrentes e devidamente comprovadas das situações previstas na alínea "d" do inciso II do art. 65 da Lei nº 8.666/1993 ou no artigo 17 do Decreto n.º 7.892/2013.

4.11.1. Nessa hipótese, o Conselho Federal de Enfermagem, por razão de interesse público, poderá optar por cancelar a Ata e iniciar outro processo licitatório.

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

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

4.13. Quando o preço de mercado tornar-se superior aos preços registrados e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

4.13.1. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, e sem aplicação da penalidade se confirmada a veracidade dos motivos e comprovantes apresentados; e

4.13.2. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

4.14. Não havendo êxito nas negociações previstas na Condição anterior, o órgão gerenciador deverá proceder à revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

4.15. O registro do fornecedor será cancelado quando:

4.15.1. Descumprir as condições da Ata de Registro de Preços;

4.15.2. Não assinar o contrato ou retirar a nota de empenho no prazo estabelecido pela Administração, sem justificativa aceitável;

4.15.3. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado; ou

4.15.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 87 da Lei n.º 8.666, de 1993, ou no art. 7º da Lei n.º 10.520, de 2002.

4.16. O cancelamento do registro de preços nas hipóteses previstas no item 4.15.1, 4.15.2 e 4.15.4 será formalizado por despacho do órgão gerenciador, assegurado o contraditório e a ampla defesa.

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

4.17.1. por razão de interesse público; ou

4.17.2. a pedido do fornecedor.

4.18. Em qualquer das hipóteses anteriores que impliquem a alteração da Ata registrada, concluídos os procedimentos de ajuste, o Conselho Federal de Enfermagem fará o devido apostilamento da Ata de Registro de Preços e informará aos fornecedores registrados a nova ordem de classificação.

4.19. A Ata de Registro de Preços, decorrente desta licitação, será cancelada, automaticamente, por decurso do prazo de sua vigência.

5. DAS OBRIGAÇÕES DA CONTRATADA E DO CONTRATANTE

5.1. As obrigações das partes estão descritas nos itens 4 e 5 do Termo de Referencia, anexo I do edital, respectivamente, que faz parte integrante do presente instrumento independentemente de transcrição.

6. RESCISÃO CONTRATUAL

6.1. A inexecução total ou parcial do objeto desta Ata de Registro de Preços, enseja a sua rescisão, conforme disposto nos artigos 77 a 80 da Lei n.º 8.666/93.

6.2. A rescisão pode ser:

6.2.1. Determinada por ato unilateral e escrito do COFEN, nos casos enumerados nos incisos I a XII e XVII do artigo 78 da Lei mencionada;

6.2.2. Amigável, por acordo entre as partes, reduzida a termo no processo de licitação, desde que haja conveniência para o COFEN;

6.2.3. Judicial, nos termos da legislação.

6.3. A rescisão administrativa ou amigável deve ser precedida de autorização escrita e fundamentada da autoridade competente.

6.3.1. Os casos de rescisão contratual devem ser formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

7. DAS PENALIDADES

7.1. As Sanções Administrativas as quais estão sujeitas a licitante vencedora, estão estabelecidas no Item 10 do Termo de referencia, anexo I do edital.

8 - DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO AO EDITAL E AO CONTRATO

8.1. A presente ata de registro de preços fundamenta-se na Lei n.º 8.666/1993, no Decreto nº 7892/2013, e vincula - se ao Edital e anexos do Pregão Eletrônico SRP - nº 17/2017, bem como à proposta da CONTRATADA, constantes do PAD n.º 40/2015, independentemente de transcrição.

9 - DOS CASOS OMISSOS.

9.1 Os casos omissos ou situações não explicitadas nas cláusulas deste Instrumento serão decididos pelo COFEN, segundo as disposições contidas na Lei nº. 8.666/93 e suas alterações posteriores e demais regulamentos e normas administrativas que fazem parte integrante desta Ata, independente de suas transcrições.

10 – DO FORO

10.1 - Fica eleito o foro da cidade de Brasília, com exclusão de qualquer outro, para dirimir qualquer questão decorrente da utilização desta Ata.

E, por se acharem as partes justas e compromissadas, assinam a presente Ata.

Brasília, _____ de _____ de 2017.

_____	_____
CONTRATANTE	CONTRATADA
MANOEL CARLOS NERI DA SILVA	
Presidente	

CONTRATANTE
JEBSON MEDEIROS DE SOUZA
1º Tesoureiro

ALBERTO JORGE SANTIAGO CABRAL
Procurador Geral

TESTEMUNHAS: