EDITAL DE LICITAÇÃO

PROCESSO n. 039/2017
PREGÃO nº 001/2018

O CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO DE JANEIRO – CREMERJ, torna público que se encontra aberta, nesta autarquia, licitação na modalidade pregão presencial, tipo menor preço, a ser realizada no dia **30 de agosto de 2018, às 10h30min.**, na sede do CREMERJ, situada à Praia de Botafogo 228/119B, Botafogo, Rio de Janeiro/RJ, CEP 22.250-145, em sessão pública, pelo pregoeiro e equipe de apoio em conformidade com as disposições da Lei nº 10.520, de 17 de julho de 2002, pelos Decretos 3.555/2000, Decreto 7.892/2013 e Lei Complementar nº 123, de 14 de dezembro de 2006, Lei nº 8.666, de 21 de junho de 1993 e suas alterações e demais normas regulamentares aplicáveis à espécie, bem como as condições estabelecidas a seguir.

1. OBJETO

1.1 O presente certame tem como objeto a **aquisição de solução de segurança da rede de dados do Conselho Regional de Medicina do Estado do Rio de Janeiro - CREMERJ, composta por elementos de hardware e software, incluindo licenciamento, instalação, garantia e suporte técnico**, conforme especificações definidas no Termo de Referência, parte integrante deste Edital.

ITEM	ESPECIFICAÇÃO	QUANTIDADE
01	WatchGuard Firebox M570 Series Hardware - PN WGFBM570HW	01 (Um)
02	Trade Up to WatchGuard Firebox M570 with 3-yr Total Security Suite (Software Only) - PN WGTM570MD3TU	01 (Um)
03	WatchGuard Firebox AP320 Hardware - PN WGAP320HW	05 (Cinco)
04	WatchGuard AP320 and 3-yr Standard Support - PN WGLAP320MD3	05 (Cinco)
05	WatchGuard AP200 1-yr LiveSecurity Renewal PN WG019818	07 (Sete)
06	Instalação física e Configuração • Instalação física de todos os equipamentos; • Atualização de Firmware da Solução de Segurança de todos os equipamentos; • Configuração de ambiente de segurança aderente às políticas do cliente de todos os hardwares; • Configuração de Servidor de Relatórios; • Passagem de conhecimento para a equipe; • Documentação;	01 (Um)

1.2 São partes integrantes deste Edital, os seguintes anexos:

ANEXO I – MODELOS DE DOCUMENTOS

- PROCURAÇÃO – CREDENCIAMENTO;
- MODELO DE DECLARAÇÃO EM ATENDIMENTO AO INCISO V, ARTIGO 27 DA LEI N.º 8.666/93;
- MODELO DE DECLARAÇÃO EM ATENDIMENTO AO INCISO VII, ARTIGO 4º DA LEI Nº 10.520, DE 17 DE JULHO DE 2002, DE QUE CUMPRE PLENAMENTE OS REQUISITOS DE HABILITAÇÃO E SE SUJEITA AS REGRAS DO PRESENTE PREGÃO;
- MODELO DE DECLARAÇÃO DE ME/EPP;
- MODELO DE DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO;
- MODELO DE ATESTADO DE CAPACIDADE TÉCNICA;
- MODELO DE DECLARAÇÃO QUE POSSUI TOTAL CONHECIMENTO DO OBJETO DA PRESENTE LICITAÇÃO E ATENDE AO DISPOSTO NO INCISO XXXIII DO ART.7º DA CONSTITUIÇÃO FEDERAL DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988.

ANEXO II – TERMO DE REFERÊNCIA

ANEXO III – MODELO DE PROPOSTA DE PREÇOS

ANEXO IV – MINUTA DE CONTRATO

2 - DA SOLICITAÇÃO DE INFORMAÇÕES E IMPUGNAÇÕES AO EDITAL

2.1 A Pregoeira prestará todos os esclarecimentos solicitados e responderá às impugnações protocolizadas de acordo com o disposto no artigo 12 do Decreto nº 3.555 de 08.08.00, até (02) dois dias úteis antes da data fixada para recebimento das propostas, ou seja, até **27/08/18**.

2.1.1 As solicitações de esclarecimentos de dúvidas, de providências ou impugnação deverão ser dirigidas à Pregoeira e protocolizadas na Recepção do CREMERJ, situada na Praia de Botafogo, 228, Lj. 119B - Botafogo, Rio de Janeiro/RJ, CEP 22.250-145, no horário de 11h às 16h, **ou** através do e-mail licitacoes@crm-rj.gov.br, até às 16h do prazo final, conforme estipulado no artigo 12, *caput*, do Decreto nº 3.555/00 *(Até dois dias antes da data fixada para recebimento das propostas).*

2.2. O licitante se obriga a verificar todas e quaisquer informações, tais como, respostas a pedidos de esclarecimentos, impugnações, entre outras, sobre o presente certame no site do CREMERJ: www.cremerj.org.br, no link “Institucional”, “Licitações”, “Pregão” e selecionar o pregão no qual está participando.

2.3. O CREMERJ poderá, também, por iniciativa própria e a qualquer tempo, antes da data marcada para o recebimento dos Documentos e Propostas, transmitir informações e instruções que julgue oportunas, para a perfeita e correta interpretação das condições deste Pregão. Tais

informações estarão disponíveis no site do CREMERJ e o licitante fica responsável por acessá-lo e obter todas as informações do certame.

2.4 Não deverão ser considerados, pelos participantes, na formulação de suas Propostas, quaisquer esclarecimentos e/ou informações obtidos de forma diferente da estabelecida no Item **2.2** deste Edital.

3 - DAS CONDIÇÕES GERAIS PARA PARTICIPAÇÃO

3.1 As empresas que desejarem participar deste Pregão deverão, no dia, hora e local estabelecidos neste edital, depois de declarada aberta a sessão:

a) proceder ao credenciamento na forma do *Capítulo V – DO CREDENCIAMENTO*;

b) entregar os envelopes: **separados**, **lacrados**, **invioláveis** e **não transparentes** da "PROPOSTA COMERCIAL" e "HABILITAÇÃO", contendo na parte externa: o nº do processo, nº do pregão, nome da empresa com o respectivo nº de inscrição no CNPJ, local, data e hora da realização do certame, não sendo permitida a entrega dos envelopes em nenhum outro momento.

c) Em conformidade com o art. 49, III da Lei 123/2006, o objeto não será divisível, por ser de alta complexidade o objeto e para que haja sucesso na totalidade da sua execução.

3.2 Não poderão participar:

a) empresas que estejam declaradas inidôneas para licitar ou contratar com a Administração Pública ou suspensas de participar em licitação e impedidas de contratar com o CREMERJ, como previsto no art. 87, III e IV, da Lei nº 8.666/93;

b) empresas com falência decretada ou em recuperação judicial ou extrajudicial;

c) consórcio de empresas, qualquer que seja sua forma de constituição;

d) servidores ou dirigentes deste órgão, conforme art. 9º, III, da Lei nº 8666/93;

e) Não será permitida a participação de empresas distintas através de um único representante.

3.3 Para fins de comprovação do atendimento das alíneas "**a**" e "**b**", adicionalmente aos documentos exigidos, serão efetuadas as seguintes diligências, ambas visando comprovar a regularidade da licitante, antes da assinatura contratual, junto ao:

a) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa,

mantido pelo Conselho Nacional de Justiça - CNJ, nos termos do art. 12 da Lei n.º 8.429/1992, disponível por meio de consulta ao site www.cnj.jus.br;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS), disponível no endereço eletrônico www.portaldatransparencia.gov.br/ceis/Consulta.seam.

4 – DA AUTENTICAÇÃO

4.1. A autenticação de documentos pelo CREMERJ, caso necessário pelos Licitantes, poderá ser requisitada na sede do órgão situado à Praia de Botafogo, 228/Loja 119 B – Botafogo – Rio de Janeiro/RJ, CEP: 22.250-145, no período de 10:30h às 11:00h no dia marcado para recebimento das Propostas constante do preâmbulo deste Edital, perante ao Pregoeiro e Equipe de Apoio.

5 - DO CREDENCIAMENTO

5.1 Cada empresa licitante far-se-á representar por seu titular ou pessoa devidamente credenciada, e somente este poderá atuar na formulação de propostas e na prática de todos os demais atos inerentes ao certame. No ato da Sessão Pública serão efetivadas as devidas comprovações quanto à existência dos necessários poderes para a representação ou credenciamento através da apresentação dos documentos abaixo indicados, fora dos envelopes e nos moldes da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil Brasileiro).

5.2 A empresa deverá apresentar, no momento do Credenciamento:

5.2.1 Cópia simples do documento de constituição, na forma do **subitem 5.2.2**, onde conste, dentre os objetivos sociais, a execução de atividade da mesma natureza ou compatível com o objeto da licitação.

5.2.2 Se a empresa se fizer representar por seu sócio, deverá este, para que se promovam as devidas averiguações quanto à administração e gerência da sociedade, apresentar Carteira de Identidade ou documento equivalente, Ato Constitutivo, Estatuto ou Contrato Social, devidamente registrado, em se tratando de sociedades empresárias, e, no caso de sociedades por ações, acompanhado de documento de eleição de seus administradores, ou no caso de empresa individual, o registro comercial. No caso de sociedades simples, a inscrição do ato constitutivo, acompanhado de prova de diretoria em exercício. Para o credenciamento, poderá ser utilizada cópia simples destes documentos.

5.2.3 Os documentos referidos na cláusula 5.2.2 deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

5.2.4 Declaração dando ciência de que cumprem plenamente os requisitos de habilitação constantes neste edital, conforme art. 4º, inc. VII da Lei nº 10.520, de 17 de julho de 2002 (Anexo I);

5.2.5 Declaração de ME/EPP (modelo no anexo I), caso a empresa se enquadre nesta situação.

5.2.5.1 A microempresa ou empresa de pequeno porte deverá apresentar declaração, sob as penas da lei, de que cumpre os requisitos legais para a qualificação como microempresa ou empresa de pequeno porte, estando apta a usufruir do tratamento favorecido pelas Leis Complementares n. 123/2006 e 147/2014, bem como de que não incide em qualquer das vedações estabelecidas no art. 3º, § 4º, da Lei Complementar n. 123/2006.

5.2.6 Caso seja designado outro representante, este deverá estar devidamente credenciado, tendo como condição para que o credenciamento seja aceito a apresentação dos seguintes documentos:

a) Carteira de Identidade ou documento equivalente;

b) Procuração/Carta de Credenciamento, assinada pelo representante legal da empresa, nos termos do seu Ato Constitutivo, Estatuto ou Contrato Social, documento esse a ser entregue visando à comprovação da condição do titular para delegar poderes ao representante a ser credenciado, ou instrumento público de mandato;

b.1) O instrumento particular de mandato deverá obrigatoriamente estar com a firma reconhecida, de acordo com o disposto no § 2º do art. 654 do Código Civil Brasileiro.

5.3 Ficam as empresas cientes de que somente participarão da fase de lances verbais aquelas que se encontrarem devidamente credenciadas nos termos do Capítulo V. As licitantes que decidirem pelo envio dos envelopes, sem que se efetive o devido credenciamento, somente participarão do certame com o preço constante no envelope da proposta comercial.

5.4 Finalizada a fase de credenciamento pelo Pregoeiro, não mais serão admitidos novos proponentes.

5.5 Após o credenciamento, os proponentes somente poderão se ausentar do local do Pregão com a prévia anuência do Pregoeiro, sob pena de sua exclusão do certame.

5.6 Todos documentos necessários ao Credenciamento acima listados, devem ser apresentados com **cópia e original ou por cópia autenticada** para a devida conferência.

5.6.1 Os documentos **constantes do Item 5.2.4, 5.2.5 e os documentos constantes das alíneas a, b do Item 5.2.6** acima mencionados, devem ser entregues ao pregoeiro no Ato

do Credenciamento**, em caráter definitivo,** para fins de juntada aos autos do processo licitatório, conforme especificado abaixo;

a) O documento constante na alínea ***a*** do **Item 5.2.6** (*Identidade ou documento equivalente)* deve ser apresentado: através de cópia (indispensável original para conferência no ato do credenciamento);

b) Os documentos constantes dos **itens 5.2.4, 5.2.5** e os documentos constantes na alínea ***b*** do **item 5.2.6** *(Procuração/Carta de Credenciamento e Declarações)* devem ser apresentados: através de originais.

6 - DA PROPOSTA COMERCIAL

6.1 A proposta comercial deverá ser apresentada em envelope indevassável, constando da parte externa as indicações descritas no **subitem 3.1.”b”**.

6.1.1 É vedado ao licitante desistir da proposta após a abertura do primeiro envelope de preços de qualquer licitante.

6.2 A proposta comercial deverá ser apresentada no original, **preferencialmente,** no modelo constante do ANEXO III deste Edital, minuciosamente descrita e impressa em via única, datada, assinada pelo representante legal ou procurador da empresa, devidamente identificado com o nome, número da identidade e cargo, sem emendas, rasuras ou entrelinhas, contendo ainda o nome, endereço atual completo e nº do CNPJ da proponente.

6.3 Ao apresentar sua proposta e ao formular lances, o licitante concorda especificamente com as seguintes condições:

a) a proposta de preços englobará todas as despesas diretas e indiretas incidentes ou relacionadas com a entrega do objeto. Nenhuma reivindicação adicional de pagamento ou reajustamento de preços será considerada;

b) a proposta de preços deverá ser válida pelo período de, no mínimo, 60 (sessenta) dias**,** contados a partir da data prevista para abertura do certame;

c) é vedada qualquer indexação de preços por índices gerais, setoriais ou que reflitam a variação dos custos.

6.3.1 Caso a licitante não informe em sua proposta comercial o prazo de validade da proposta, será considerado o estabelecido na letra “b” do subitem **6.3.**

6.4. A empresa vencedora, tendo ofertado lance durante a sessão, deverá apresentar nova planilha a que se refere o subitem 6.2, até o 5º (quinto) dia útil subsequente à data da

realização do certame, através de correio eletrônico, pelo e-mail licitacoes@crm-rj.gov.br ou através de entrega no Setor de Licitações, Compras e Contratos do CREMERJ, com endereço à Praia de Botafogo, n. 228 – loja 119B – Botafogo – Rio de Janeiro/RJ, CEP 22.250-145, no horário de 9:00h às 18:00h.

6.5 Os erros ou equívocos porventura ocorridos nas cotações serão de inteira responsabilidade do proponente.

6.6. Havendo discordância entre os preços unitário e total, prevalecerá o primeiro, e entre os valores expressos em algarismos e por extenso, serão considerados estes últimos, devendo a Pregoeira proceder às correções necessárias.

7 - DO JULGAMENTO DAS PROPOSTAS

7.1. Após realização de pesquisa de mercado, no julgamento das propostas será adotado o critério do tipo MENOR PREÇO GLOBAL *(representado pela soma dos valores dos Itens 1, 2, 3, 4, 5 e 6)*, devendo ser considerada como **valor máximo unitário por item a ser ofertado pelo Licitante,** aqueles constantes da tabela abaixo:

ITEM	OBJETOS	QUANT.	VALOR MÁX. UNIT.	VALOR MÁX. GLOBAL
1	WatchGuard Firebox M570 Series Hardware - PN WGFBM570HW	01 (Um)	**R$ 8.836,88**	**R$ 8.836,88**
2	Trade Up to WatchGuard Firebox M570 with 3-yr Total Security Suite (Software Only) - PN WGTM570MD3TU	01 (Um)	**R$ 119.854,72**	**R$ 119.854,72**
3	WatchGuard Firebox AP320 Hardware - PN WGAP320HW	05 (Cinco)	**R$ 1.536,70**	**R$ 7.683,50**
4	WatchGuard AP320 and 3-yr Standard Support - PN WGLAP320MD3 R	05 (Cinco)	**R$ 3.525,87**	**R$ 17.629,35**
5	WatchGuard AP200 1-yr LiveSecurity Renewal PN WG019818	07 (Sete)	**R$ 4.455,05**	**R$ 31.185,35**
6	- Instalação física - Atualização de Firmware da Solução de Segurança - Configuração de ambiente de segurança aderente às políticas do cliente - Configuração de Servidor de Relatórios;	01 (Um)	**R$ 9.346,67**	**R$ 9.346,67**
VALOR MÁXIMO GLOBAL = (Soma dos valores dos itens 1 + 2 + 3 + 4 + 5 + 6)				**R$ 194.536,47**

7.2. Será verificada a conformidade das propostas apresentadas com os requisitos estabelecidos neste Instrumento Convocatório, sendo desclassificadas as propostas:

7.2.1. Que apresentarem valores unitários por item superiores aos informados na tabela constante no **Item 7.1.;**

7.2.2. Que apresentarem valor máximo global superior ao informado (soma dos Itens 1+2+3+4+5+6) no **Item 7.1.**, ou seja, **superior a R$ 194.536,47 (Cento e noventa e quatro mil e quinhentos e trinta e seis reais e quarenta e sete centavos)**.

7.3. Serão classificados pela Pregoeira os proponentes que apresentarem as propostas do tipo MENOR PREÇO TOTAL, em conformidade com a descrição do objeto, em especial, constante do **subitem 1.1.** e **7.1** deste Edital, assim como do Termo de Referência, anexo II deste Edital.

7.4. Caso duas ou mais propostas iniciais apresentem preços iguais, será realizado sorteio para determinação da ordem de oferta dos lances.

7.5. Não serão aceitas propostas que apresentarem preços globais simbólicos, irrisórios ou de valor zero.

7.6. Não poderá haver desistência dos lances ofertados, sujeitando-se o proponente desistente às penalidades constantes do Capítulo XIII, deste Edital.

7.7. A desistência em apresentar lance verbal, quando convocado pela Pregoeira, implicará a exclusão da licitante da etapa de lances verbais e a manutenção do último preço apresentado pela empresa para efeito de ordenação de propostas.

7.8. A Pregoeira examinará a aceitabilidade, quanto ao objeto e valor, da primeira classificada, decidindo motivadamente a respeito. Se a oferta não for aceitável, a Pregoeira poderá negociar diretamente com o proponente para que seja obtido um preço melhor.

7.9. Sendo aceitável o menor preço ofertado, e estando a especificação da proposta de acordo com o Edital, a Pregoeira verificará o atendimento das condições habilitatórias pelo licitante que a tiver formulado.

8 – DA HABILITAÇÃO

8.1 Os documentos de habilitação deverão ser apresentados em envelope indevassável, constando da parte externa as indicações descritas no item 3.1. “b”, contendo:

8.2 DAS DOCUMENTAÇÕES PARA HABILITAÇÃO *(Envelope lacrado)*

8.2.1 Documentação relativa à HABILITAÇÃO JURÍDICA:

a) Registro Comercial, no caso de empresário individual;

b) Ato Constitutivo, Estatuto ou Contrato Social, devidamente registrado, em se tratando de sociedades empresárias, e, no caso de sociedades por ações, acompanhado de documento de eleição de seus administradores. No caso de sociedades simples, a inscrição do ato Constitutivo, acompanhado de prova de diretoria em exercício no caso de S.A;

b.1) Nos casos de registros oriundos da JUCERJA (Junta Comercial do Estado do Rio de Janeiro – Deliberação JUCERJA n. 74/2014) ou de outra Junta Comercial, desde que tenham deliberado no mesmo sentido, poderá haver abstenção da autenticação cartorial face a utilização de *chancela digital*;

c) Decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no país, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

c.1) Os documentos referidos acima **deverão estar acompanhados de todas as alterações ou da consolidação respectiva**, através de cópia autenticada por cartório competente ou pelo CREMERJ.

d) Declaração em atendimento ao inciso V, artigo 27 da lei n.º 8.666/93 (modelo no anexo I).

e) Declaração de inexistência de fato impeditivo (modelo no anexo I).

8.2.3 Documentação relativa à REGULARIDADE FISCAL:

a) Prova de Inscrição no Cadastro Nacional de Pessoa Jurídica (CNPJ), do Ministério da Fazenda;

b) Prova de Inscrição no Cadastro de Contribuintes Estadual ou Municipal, se houver, relativo à sede da licitante, pertinente ao seu ramo de atividade e compatível com o objeto deste edital;

c) Prova de Regularidade para com a Fazenda Estadual e Municipal da sede do licitante, ou outra equivalente, na forma da lei;

d) Prova de Regularidade relativa à Seguridade Social (INSS) e ao Fundo de Garantia por Tempo de Serviço (FGTS);

e) Prova de Regularidade para com a Fazenda Federal, Receita Federal do Brasil (*Consolidada conforme Portaria nº 1751 de 02/10/14, da Secretaria da Receita Federal, publicada no DOU na Seção 1 em 03/10/14)*;

f) Prova de regularidade relativa à Justiça do Trabalho por meio da apresentação da Certidão Negativa de Débitos Trabalhistas (CNDT) em plena validade.

8.2.4 Documentação relativa à QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

a) Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de três meses da data da apresentação da proposta:

a.1) Será considerado último exercício social a data base de entrega do SPED contábil da Secretaria da Receita Federal.

a.2) Serão considerados aceitos como na forma da lei o balanço patrimonial e demonstrações contábeis, a depender da forma de constituição, assim apresentados:

1-1 Sociedades empresariais em geral: registrado ou autenticado no órgão de Registro do comércio da sede ou do domicílio da Licitante, acompanhado de **cópia do termo de abertura e de encerramento do Livro Diário do qual foi extraído;**

1-2 Sociedades empresárias, especificamente no caso de sociedades anônimas- S.A.: regidas pela Lei nº 6.404/1976: registrado ou autenticado no órgão de Registro do Comércio da sede ou domicílio da Licitante e publicado em Diário Oficial ou em Jornal de grande circulação ou fotocópia registrada ou autenticada no órgão competente de Registro do Comércio da sede ou domicílio da Licitante acompanhado **de cópia do termo de abertura e encerramento do livro diário do qual foi extraído;**

1-3 Sociedades Simples: registrado no Registro Civil das Pessoas Jurídicas do local de sua sede acompanhado **de cópia do termo de abertura e encerramento do livro diário do qual foi extraído**; caso a sociedade simples adote um dos tipos de sociedade empresária, deverá sujeitar-se às normas fixadas para as sociedades empresárias, inclusive quanto ao registro no órgão de Registro do Comércio;

1-4 As **Empresas constituídas no exercício em curso ou com menos de um ano**: deverão apresentar balanço conforme abaixo discriminado, com a assinatura do sócio- gerente e do responsável por sua contabilidade e a indicação do nome deste e do seu número de registro no Conselho Regional de Contabilidade ou equivalente, devidamente registrado ou autenticado no

órgão de Registro do Comércio da sede ou do domicílio da Licitante: a) balanço de abertura, no caso de sociedades sem movimentação; b) balanço intermediário, no caso de sociedades com movimentação;
1-5 Por cópia do SPED Contábil, devidamente autenticada através de emissão no sítio eletrônico: www.receita.fazenda.gov.br

a.3) O balanço patrimonial do último exercício social não será exigido da microempresa e da empresa de pequeno porte, somente no caso descrito no art. 3º do Decreto Federal n. 8538/2015, conforme abaixo:

"Na habilitação em licitações para o fornecimento de bens para pronta entrega ou para a locação de materiais, não será exigida da microempresa ou da empresa de pequeno porte a apresentação de balanço patrimonial do último exercício social".

b) Certidão Negativa de Falência ou Recuperação Judicial ou Extrajudicial expedida pelo distribuidor da sede da pessoa jurídica, datada de até 90 (noventa) dias anteriores à data marcada para esta licitação;

c) A boa situação financeira de todas as licitantes será avaliada pelos Índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), iguais ou maiores que 1 (um), resultantes da aplicação das fórmulas abaixo, com os valores extraídos de seu balanço patrimonial:

$$LG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + EXIGÍVEL A LONGO PRAZO}}$$

$$LC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}}$$

c.1) Do balanço referido na alínea c do Item 8.2.4, cujo índice de solvência, obtido conforme fórmula acima, terá de ser maior ou igual a um (≥ a 1).

d) A licitante, cadastrada ou não no SICAF, que apresentar índices econômicos iguais ou inferiores a 01 (um) em qualquer dos índices de Liquidez Geral, Solvência Geral e Liquidez Corrente, deverá comprovar que possui capital social mínimo ou patrimônio líquido mínimo de 10% (dez por cento) do valor estimado do item.

e) As licitantes deverão comprovar a sua regularidade mediante a apresentação das Certidões Negativa de Débito (CND´s), em conformidade com o disposto no inciso XIII, do artigo 4º, da lei 10.520/02.

8.2.5 Documentação relativa à QUALIFICAÇÃO TÉCNICA (Modelos no Anexo I):

a) Atestado de Capacidade Técnica, fornecido por pessoa jurídica de direito público ou privado, comprovando que a licitante executou de forma satisfatória os serviços com características pertinentes e compatíveis com as previstas na presente licitação;

b) Declaração contendo o seguinte teor:

b.1) de que possui total conhecimento do objeto da presente licitação e que cumpre o disposto no inciso XXXIII do artigo 7º da Constituição da República Federativa do Brasil de 1988;

b.2) que cumprirá os prazos exigidos para o fornecimento dos itens de produto/software que são objeto deste certame.

8.3 Os documentos referidos no subitem 8.2.5 alíneas "b.1" e "b.2" deverão ser em originais e assinados por sócio, diretor ou representante legal da licitante, observado o item 5.1 deste Edital.

8.4 Os documentos exigidos poderão ser analisados pelo gestor/fiscal do futuro contrato para emissão de parecer técnico em eventual diligência instaurada pela Pregoeira, a qual poderá considerá-lo no julgamento da habilitação, conforme artigo 43, § 3º da Lei 8.666/93.

8.5 O CREMERJ poderá promover visita às dependências da Licitante e consulta às entidades competentes, a fim de comprovar a exatidão das informações contidas nos documentos requeridos.

8.6 A Pregoeira reserva-se o direito de solicitar da Licitante, em qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre documentos já entregues, fixando-lhe prazo para atendimento.

8.7 Serão inabilitadas as empresas licitantes que não apresentarem a documentação em situação regular, observado o disposto no art. 4º §1º do Decreto nº 8.538/2015 no que diz respeito às microempresas e empresas de pequeno porte.

8.8 A falta de quaisquer dos documentos exigidos no edital, implicará inabilitação da licitante, sendo vedada, sob qualquer pretexto, a concessão de prazo para complementação da documentação exigida para a habilitação, ressalvada a hipótese prevista no **item 8.9** deste Edital.

8.9 No caso de microempresa ou empresa de pequeno porte que esteja com alguma **restrição na comprovação da REGULARIDADE FISCAL**, será assegurado o **PRAZO DE 05 (CINCO) DIAS ÚTEIS**, conforme art. 43, §1º da lei Complementar 123/2006, cujo termo inicial corresponderá

ao momento em que o PROPONENTE (ME ou EPP) foi declarado vencedor do certame, prorrogáveis por igual período, quando requerido pelo licitante e a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

8.9.1 A não regularização da documentação no prazo previsto no **item 8.9**, implicará decadência do direito à contratação, sem prejuízo das sanções previstas na lei, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para a assinatura do contrato, ou revogar a licitação.

8.10 Todos os documentos exigidos neste edital deverão ser apresentados em originais ou por cópias reprográficas, obrigatoriamente autenticadas de acordo com o artigo 32 da Lei nº 8.666/93.

8.11 Se houver impossibilidade de apresentar qualquer documento por motivo de greve do órgão emissor, deverá o licitante apresentar declaração em papel timbrado da empresa, assinado por seu representante legal, de que não está em débito com o referido órgão e que, finda a greve, se compromete a apresentar o documento atualizado, para fins de direito, em até 10 (dez) dias úteis, independentemente da fase em que se encontrar o processo licitatório, sujeitando-se, no caso de não apresentação, às penalidades legais, nos termos do Capítulo XIII deste Edital.

8.12 No caso de inabilitação do proponente que tiver apresentado a melhor oferta, a Pregoeira examinará as condições de habilitação da proposta classificada em segundo lugar, e assim sucessivamente, até que uma licitante atenda às condições fixadas neste Edital.

8.13 Verificado o atendimento pleno das exigências Editalícias, será declarado o proponente vencedor, sendo-lhe ADJUDICADO pela Pregoeira o objeto para o qual apresentou proposta.

8.14 A Pregoeira manterá em seu poder os documentos das demais licitantes, pelo prazo de 15 (quinze) dias, após a homologação da licitação, devendo as empresas retirá-los após este período, sob pena de inutilização dos mesmos.

8.15 Da Sessão Pública será elaborada ata circunstanciada, em que serão registradas as ocorrências relevantes e, ao final, será assinada pela Pregoeira, equipe de apoio e demais presentes.

8.16 Após o resultado da licitação e a homologação, resumo será publicado na Imprensa Oficial, para ciência dos interessados e efeitos legais.

9 – DOS RECURSOS ADMINISTRATIVOS

9.1 Declarada a empresa vencedora, qualquer licitante poderá manifestar, imediata e motivadamente, a intenção de recorrer, sendo registrada em ata a síntese das razões recursais, sendo-lhe concedido o prazo de 03 (três) dias úteis para a apresentação das razões escritas, ficando as demais licitantes, desde logo, intimadas a apresentar contrarrazões em igual número de dias, que começarão a correr do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa de seus interesses.
9.2 A falta de manifestação imediata e motivada de recorrer importará em decadência do direito de recorrer. Os recursos imotivados ou insubsistentes não serão recebidos.

9.3 O acolhimento do recurso importará a invalidação apenas dos atos insuscetíveis de aproveitamento. O recurso contra decisão do pregoeiro não terá efeito suspensivo, conforme prevê o artigo 11, inciso XVIII, do Decreto nº 3.555/00.

9.4 O recurso deverá ser dirigido à Pregoeira e protocolizado na Recepção do CREMERJ, situada na Praia de Botafogo, 228, Botafogo, Rio de Janeiro/RJ, no horário de 11h às 16h, dentro do prazo estabelecido no item 9.1.

10 - DA HOMOLOGAÇÃO

10.1 Não sendo interposto recurso, caberá à Autoridade Competente adjudicar o objeto e ao Presidente do CREMERJ, homologar o procedimento licitatório.

10.2 Havendo recurso, a Administração do CREMERJ, após deliberar sobre o mesmo, fará a adjudicação do objeto, homologando ou não o procedimento licitatório.

11 – DO CONTRATO

11.1 Depois de homologado o certame e adjudicado o objeto pertinente, a licitante vencedora deverá comparecer ao CREMERJ para assinatura do instrumento pertinente, no prazo de até 05 (cinco) dias úteis, a contar da data de sua convocação.

11.2 A recusa do Proponente vencedor em assinar o Contrato, conforme designado por este órgão, no prazo fixado neste Edital, caracterizará inadimplência das obrigações decorrentes desta licitação, sujeitando-se às penalidades previstas neste Edital e na legislação vigente.

11.3 Ocorrendo a hipótese, o processo retornará ao Pregoeiro que convocará os Proponentes e, em sessão pública, procederá ao exame das demais Propostas, bem como da habilitação de seus ofertantes, segundo a ordem da classificação, até que uma Proposta atenda integralmente ao Edital, sendo o seu autor declarado vencedor e convocado para a devida assinatura do instrumento, nos termos da Cláusula 11.1 do presente Edital.

11.4 A empresa VENCEDORA deverá indicar na data da assinatura, preposto para representá-la durante a execução do objeto deste Edital, nos termos do art. 68 da Lei 8.666/93, bem como disponibilizar um endereço eletrônico e número de telefone local para contato imediato com o(s) Fiscal(is) do Contrato.

12 – DA RESCISÃO

12.1 A inexecução parcial ou total deste ensejará sua rescisão, com as consequências previstas em lei, conforme minuta do Contrato e legislação pertinente.

13 - DA FISCALIZAÇÃO

13.1 A fiscalização será exercida pelo(s) Fiscal(is), devidamente designado(s) pelo CREMERJ – conforme art. 67 da lei 8666/93, ao qual incumbirá acompanhar a prestação dos serviços objeto deste Edital, em sua íntegra, determinando à empresa VENCEDORA as providências necessárias ao regular e efetivo cumprimento das condições estabelecidas neste instrumento e seus anexos, bem como anotar e enquadrar as infrações constatadas, comunicando as mesmas ao seu superior hierárquico.

14 - DAS SANÇÕES ADMINISTRATIVAS

14.1 Quem, convocado dentro do prazo de validade da sua proposta, não assinar o instrumento respectivo, oriundo deste Edital e seus anexos, ou deixar de entregar documentação exigida para o certame, apresentar documentação falsa, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar a adequada execução deste objeto, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, ficará sujeito a ser impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios, e a ser descredenciado dos sistemas de cadastramento de fornecedores a que se refere o inciso XIV do art. 4º da Lei nº 10.520 de 10/07/02, pelo prazo de até 05 (cinco) anos, sem prejuízo das demais cominações legais previstas na Lei 8.666/93, assegurada a observância do prévio contraditório e da ampla defesa.

14.2 Pela inexecução parcial ou total das cláusulas avençadas, garantido o direito à ampla defesa, poderá ser aplicada à empresa VENCEDORA as sanções administrativas previstas na legislação em vigor.

14.3 A empresa VENCEDORA incorrerá em multa no percentual de até 10% (dez por cento) sobre o valor contratado do serviço, por infração de qualquer das cláusulas previstas;

14.4 As sanções previstas poderão ser registradas em sistemas de cadastramento de fornecedores.

14.5 O valor da multa, aplicada após o regular processo administrativo, será deduzida da fatura devida, ou ainda, cobrada diretamente da empresa VENCEDORA, amigável ou judicialmente, na forma dos parágrafos 2º e 3º do artigo 86 da Lei nº 8.666/93.

15 - DO PAGAMENTO

15.1 O pagamento será efetuado em até 20 (vinte) dias corridos, a contar do recebimento da Nota Fiscal devidamente discriminada em nome do Conselho Regional de Medicina do Estado do Rio de Janeiro, CNPJ n.º 31.027.527/0001-33, após a perfeita execução dos serviços contratados, constando o número do Processo (nº 039/2017) e o número do Pregão (nº 001/2018), acompanhada dos seguintes documentos, sem o qual, havendo atraso dos mesmos, ensejará a contagem de novo prazo para pagamento:

15.1.1 Declaração do Simples *(assinada e original)*, *caso a empresa seja Optantes do SIMPLES Nacional*;

15.1.2 Certidão de Regularidade do FGTS, Certidão específica quanto à inexistência de débito de contribuições junto ao INSS, Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, conforme Decreto n.º 6.106/2007, ou alterações posteriores.

15.2 O pagamento poderá ser feito através de boleto bancário ou depósito, sendo neste último caso, necessário que conste na descrição da Nota Fiscal os dados: Banco, Agência e Conta para depósito, cuja titularidade deve estar em nome da empresa vencedora deste certame licitatório.

15.3 A liberação da Nota Fiscal/Fatura para pagamento ficará condicionada ao atesto do(s) Fiscal(is), conforme disposto nos artigos 67 e 73 da Lei n. º 8.666/93;

15.4 Qualquer atraso ocorrido na apresentação dos documentos exigidos nos Itens *15.1, 15.1.1* e *15.1.2* importará em prorrogação automática do prazo de vencimento da obrigação do CREMERJ até sanada todas as pendências.

15.5 Fica o VENCEDOR ciente de que, quando da ocasião do pagamento, será verificado se as condições de habilitação estão mantidas, sem as quais ocorrerá prorrogação automática do prazo de vencimento da obrigação do CREMERJ até que a regularidade seja comprovada.

15.6 Fica a empresa VENCEDORA ciente da obrigatoriedade de apresentação do Termo de Opção pelo Simples, quando assim couber, no ato da entrega da Nota Fiscal, esclarecendo o CREMERJ que a não apresentação do documento em questão, ocasionará o desconto no pagamento devido à empresa do valor referente ao encargo previsto na Lei nº 9.430 de 27/12/96.

15.7 Todos os impostos serão retidos em conformidade com a IN-RFB nº 1.234, de 11 de janeiro de 2012 e suas alterações posteriores.

15.8 O preço ofertado na licitação para cada um dos itens será fixo e irreajustável durante a vigência contratual, cabendo a empresa VENCEDORA, mantê-lo para a execução na íntegra do objeto contratual.

16 - DAS DISPOSIÇÕES GERAIS

16.1 Fica ressalvado ao CREMERJ o direito de, por provocação ou de ofício, em razão de ilegalidade, anular, no todo ou em parte, ou revogar por interesse público a presente Licitação, bem como aumentar ou suprimir o valor do contrato, dentro dos limites fixados, em conformidade com os artigos 49 e 65, parágrafos 1º e 2º, ambos da Lei 8.666/93.

16.2 A empresa VENCEDORA fica obrigada a não transferir no todo, os produtos adjudicados, que constituem objetos desta licitação.

16.3 Ocorrendo decretação de feriado ou outro fato superveniente, de caráter público, que impeça realização do certame na data acima marcada, a licitação ficará automaticamente prorrogada para o primeiro dia útil subsequente, no mesmo horário, independente de nova comunicação, salvo aviso expresso da Autoridade Competente.

16.4 O CREMERJ se reserva ao direito de documentar a sessão com o uso de gravadores de imagem e som, inclusive usar gravações como meio de prova, administrativo e judicial.

16.5 Para a contagem dos prazos deste Edital será considerado o horário oficial de Brasília/DF.

16.6 Fica eleito o foro da Justiça Federal do Estado do Rio de Janeiro para dirimir todas as questões oriundas do presente instrumento.

Rio de Janeiro, 30 de julho de 2018.

Margareth de Souza do Espírito Santo
Pregoeira

Presidente Nelson Nahon
CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO DE JANEIRO

ANEXO I - MODELOS DE DOCUMENTOS

MODELO DE PROCURAÇÃO:

CREDENCIAMENTO

(empresa), com sede (endereço), CNPJ/MF, neste ato representada por seu (s) representante (s) legal (is) ao final assinado (s), nomeia e constitui seu bastante procurador, (nome), (qualificação), (RG), (CPF), (domicílio/residência), ao qual outorga poderes específicos para representar a Outorgante no processo licitatório, na modalidade de Pregão n.º_____/_____, junto ao Conselho Regional de Medicina do Estado do Rio de Janeiro - CREMERJ, especialmente para formular lances, manifestar intenção de interpor recurso ou renunciar ao direito de recorrer, enfim, praticar todos os atos pertinentes ao referido pregão, podendo ainda requerer, impugnar, desistir, assinar qualquer documento necessário ao fiel cumprimento deste mandato.

Rio de Janeiro, _____de _____de ____.

_____

(NOME/CARGO)

MODELO DE:

DECLARAÇÃO EM ATENDIMENTO AO INCISO V, ARTIGO 27 DA LEI N.º 8.666/93.

A empresa _____, inscrita no CNPJ sob o n.º_____, sediada na _____, por intermédio do seu representante legal o(a) Sr(a) _____, portador(a) da Carteira de Identidade n.º _____ e CPF n.º _____, DECLARA para fins do disposto no inciso V, do artigo 27, da Lei 8.666/93, acrescido pela Lei 9.854/99, que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre, e não emprega menor de 16 (dezesseis) anos.

Ressalva: Emprega menor, a partir de 14 (quatorze) anos, na condição de aprendiz: ( ) sim ( ) não.

Rio de Janeiro, ___ de _____de _____.

_____

(Licitante)

MODELO DE:

DECLARAÇÃO EM ATENDIMENTO AO INCISO VII, ARTIGO 4º DA LEI Nº 10.520, DE 17 DE JULHO DE 2002, DE QUE CUMPRE PLENAMENTE OS REQUISITOS DE HABILITAÇÃO E SE SUJEITA AS REGRAS DO PRESENTE PREGÃO.

A empresa _____, inscrita no CNPJ sob o n.º _____, sediada na _____, por intermédio do seu representante legal o (a) Sr(a) _____, portador (a) da Carteira de Identidade n.º _____ e CPF n.º _____, DECLARA, para fins do disposto no inciso VII, artigo 4º da Lei nº 10.520, de 17 de julho de 2002, que cumpre plenamente os requisitos de habilitação e se sujeita às regras do presente pregão.

Rio de Janeiro, _____de _____de ____.

_____

(Licitante)

MODELO DE:

D E C L A R A Ç Ã O – ME / EPP

.....(razão social do licitante), com endereço na ....., inscrita no CNPJ/MF sob o número ..... vem, pelo seu representante legal infra-assinado, sob pena de submeter-se à aplicação das sanções definidas nos artigos 7º e 9º, da Lei nº 10.520/03, **declarar que não incide em qualquer das vedações estabelecidas no artigo 3º, parágrafo 4º, da Lei Complementar nº 123**, de 14 de dezembro de 2006, abaixo transcritas:

Art. 3º Para os efeitos desta Lei Complementar, consideram-se microempresas ou empresas de pequeno porte a sociedade empresária, a sociedade simples e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002, devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme o caso, desde que:

[...]

"§ 4º Não se inclui no regime diferenciado e favorecido previsto nesta Lei Complementar, para nenhum efeito legal, a pessoa jurídica:

I – de cujo capital participe outra pessoa jurídica;

II – que seja filial, sucursal, agência ou representação, no País, de pessoa jurídica com sede no exterior;

III – de cujo capital participe pessoa física que seja inscrita como empresário ou seja sócia de outra empresa que receba tratamento jurídico diferenciado nos termos desta Lei Complementar, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do caput deste artigo;

IV – cujo titular ou sócio participe com mais de 10% (dez por cento) do capital de outra empresa não beneficiada por esta Lei Complementar, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do caput deste artigo;

V – cujo sócio ou titular seja administrador ou equiparado de outra pessoa jurídica com fins lucrativos, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do caput deste artigo;

VI – constituída sob a forma de cooperativas, salvo as de consumo;

VII – que participe do capital de outra pessoa jurídica;

VIII – que exerça atividade de banco comercial, de investimentos e de desenvolvimento, de caixa econômica, de sociedade de crédito, financiamento e investimento ou de crédito imobiliário, de corretora ou de distribuidora de títulos, valores mobiliários e câmbio, de empresa de arrendamento mercantil, de seguros privados e de capitalização ou de previdência complementar;

IX – resultante ou remanescente de cisão ou qualquer outra forma de desmembramento de pessoa jurídica que tenha ocorrido em um dos 5 (cinco) anos-calendário anteriores;

X – constituída sob a forma de sociedade por ações."

Rio de Janeiro, _____de _____de ____.

_____

(Licitante)

MODELO DE:

DECLARAÇÃO DE INEXISTÊNCIA DE FATO IMPEDITIVO

A empresa_____, sediada na _____declara sob as penas da Lei, que até a presente data, inexistem fatos impeditivos do direito de participar de licitações no âmbito da Administração Pública Federal, Estadual, Municipal ou do Distrito Federal, ciente da obrigatoriedade de declarar ocorrências posteriores.

Rio de Janeiro, ____ de _____ de _____.

_____

(Licitante)

MODELO DE:

ATESTADO DE CAPACIDADE TÉCNICA *(OU DECLARAÇÃO)*

Atestamos (ou declaramos) que a empresa _____, inscrita no CNPJ (MF) nº _____, inscrição estadual nº _____, estabelecida no (a) _____, executa (ou executou) serviços de _____ para este órgão (ou para esta empresa).

Atestamos (ou declaramos), ainda, que os compromissos assumidos pela empresa foram cumpridos satisfatoriamente, nada constando em nossos arquivos que a desabone comercial ou tecnicamente.

Local e data.

_____
(Assinatura e carimbo do emissor do Atestado)

Observação: Este atestado (ou declaração) deverá ser emitido em papel que identifique o órgão (ou empresa) emissor do referido atestado.

MODELO DE:

DECLARAÇÃO QUE POSSUI TOTAL CONHECIMENTO DO OBJETO DA PRESENTE LICITAÇÃO E ATENDE AO DISPOSTO NO INCISO XXXIII DO ART.7º DA CONSTITUIÇÃO FEDERAL DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988.

Declaramos que a empresa _____ _____, inscrita no CNPJ (MF) nº _____, inscrição estadual nº _____, estabelecida no (a) _____, possui total conhecimento do objeto da presente licitação e que cumpre o disposto no inciso XXXIII do artigo 7º da Constituição da República Federativa do Brasil de 1988.

Por fim, declara que cumprirá os prazos exigidos para o fornecimento do serviço objeto deste certame, não havendo qualquer inviabilidade para o início imediato após a assinatura do contrato.

Local e data,

_____
(Licitante)

Observação: Esta Declaração deve ser original e assinada por sócio, diretor ou representante legal da licitante.

ANEXO II - TERMO DE REFERÊNCIA

JUSTIFICATIVA DO PEDIDO

1.1. O CREMERJ conta com uma complexa estrutura computacional que garante o cumprimento de sua missão e demanda dos gestores do segmento de tecnologia da informação e comunicação, especial atenção ao ambiente tecnológico em um nível que propicie o bom desempenho das atividades de seu corpo funcional.

1.2. Ao longo dos anos o CREMERJ tem investido em recursos de tecnologia da informação e comunicação, de forma a assegurar o desempenho de suas atividades, possibilitando o tratamento de um grande e variado conjunto de informações.

1.3. A evolução da complexidade de demandas e soluções inerentes às atividades do CREMERJ exige uma adequação e constante atualização das medidas que visam proteger e assegurar a qualidade e desempenho dos serviços prestados.

1.4. De acordo com a norma internacional ISO IEC 27001:2006, que trata da certificação para Sistemas de Gestão de Segurança de Informação e apresentam entre seus conceitos fundamentais os três atributos básicos da informação: confidencialidade, integridade e disponibilidade, é necessário que este centro, no exercício de suas atribuições institucionais promova e mantenha ações que permitam o CREMERJ identificar, analisar e qualificar riscos que possam comprometer tais atributos.

1.5. Em decorrência disso, é fundamental a definição de estratégias que unifiquem os propósitos desses pilares da segurança da informação.

1.6. Dentre as medidas de segurança que garantem a proteção e a preservação das informações da instituição, destaca-se a utilização de uma ferramenta de Segurança de Redes (**Firewall**) no CREMERJ.

1.7. Esse mecanismo visa manter todo o ambiente computacional protegido contra ataques externos, malwares e garantir que os usuários dos sistemas de tecnologia do CREMERJ naveguem na internet de forma segura.

1.8. Atualmente, a solução de Firewall e Wireless é composta de interface centralizada de gerenciamento, compondo uma solução integrada de segurança e gerenciamento de rede wireless.

1.9. A interface centralizada é responsável por gerenciar os serviços de bloqueio de ameaças de segurança no parque computacional da instituição, além de controlar o tráfego da rede sem fio (*Wifi – Wireless Fidelity,* que significa fidelidade sem fio).

1.10. No processo de análise da viabilidade de substituição completa da solução atual por outra disponível no mercado verificou-se que tal processo implicaria em realizar mudança no ambiente de redes do CREMERJ, além de modificar a forma de gerenciamento, operação e monitoramento de falhas e ocorrência e tratamento de problemas.

1.11. Ademais, um processo de migração deste tipo de solução apresenta alto grau de complexidade e risco, além de demandar tempo considerável de planejamento e execução, tendo em vista a quantidade

de regras e políticas configuradas na solução já em uso no CREMERJ, além da possibilidade de desencadear problemas na implantação local, e aumentar, de forma preponderante, os riscos de operação do serviço. Desta forma, podemos mitigar o risco a partir do momento que o processo de exportação e importação das regras já existentes na solução atual poderá ser feito para o novo hardware do mesmo fabricante reduzindo muito o risco do projeto.

1.12. A ocorrência de falhas em um processo de aquisição de outros modelos poderia vir a causar impactos significativos na disponibilidade, performance e continuidade dos serviços, além de instabilidade nas aplicações em uso no CREMERJ.

1.13. A mudança completa da solução além de representar um considerável risco de instabilidade operacional, demandaria custos diretos e indiretos. Dentre os custos diretos citamos a substituição dos equipamentos atuais de *Access Points*, o próprio processo de migração, a substituição da interface central de gerenciamento e a transferência de tecnologia para que a equipe técnica pudesse absorver e se capacitar a gerenciar a nova solução. Dentre os custos indiretos, citamos os impactos nos serviços de Tecnologia da Informação e Comunicação decorrentes das interrupções em função da execução do processo de instalação e de configuração da nova solução, impactos nas rotinas operacionais dos usuários e nos projetos, haja vista a necessidade de dedicação exclusiva de parte da equipe de infraestrutura e suporte nas atividades de migração.

1.14. Ante o exposto, observando o princípio da economicidade, chegou-se à conclusão de que a continuidade do fabricante da solução atual e a expansão da solução de Access Points adicionais integráveis à solução atualmente em funcionamento no CREMERJ se apresentam como a alternativa mais segura e adequada à garantia e evolução da confiabilidade, disponibilidade e segurança dos serviços de TIC utilizados no CREMERJ. Além disso, mitigam-se os riscos que a existência de equipamentos não configurados com o programa de antivírus traz a uma rede corporativa complexa e fundamental na sustentação dos projetos, programas e atividades finalísticas que compõem a missão do CREMERJ.

1.15. Conforme observa Marçal Justen Filho, a padronização é regra. No caso, a Administração deverá ter em vista aquisições passadas e futuras. A padronização aplica-se não apenas a uma compra específica, especialmente quando se trate de bem de vida útil continuada. Ao selecionar o fornecedor para produtos não consumíveis, a Administração deverá ter em vista produto semelhante que já integram o patrimônio público, como também deverá prever eventuais futuras aquisições. Somente assim a padronização produzirá os efeitos desejados, consistentes na redução de custos de manutenção, simplificação de mão-de-obra etc (JUSTEN FILHO, 2011, p. 184).

1.16. Além do supracitado é importante observar que a solução atual além de ter findado o seu contrato, tem apresentado conforme laudo técnico em anexo um gargalo sentido pelos usuários durante o decorrer do dia.

1.17. Outro fato notório que em virtude da categoria de vírus *ransomware* (é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário) que vem assolando o mundo inteiro faz-se necessário uma proteção mais elevada, proteção essa não evidenciada na solução atual modelo WatchGuard XTM545 que segundo o site do fabricante deixou de ser comercializado em Dezembro de 2015 e está em processo de *end of life*.

1.18. Assim, faz-se necessária a aquisição de solução de segurança da rede de dados do Conselho Regional de Medicina do Estado do Rio de Janeiro, mantendo o fabricante da solução atual que é WatchGuard a fim de termos os ganhos e os riscos mitigados evidenciados acima, além da economia em não substituir os atuais *Access Point* (AP). A contratação será composta por elementos de hardware e software, incluindo licenciamento, garantia e suporte técnico, estando cobertas por 36 (trinta e seis) meses garantindo que todo o ambiente do CREMERJ tenha acesso às atualizações diárias de vacinas, versões do produto e de novos módulos, com suporte técnico especializado quando da ocorrência de incidentes ou falhas.

1.19. Com o objetivo de ampliar a quantidade de *Access Point* (AP) no CREMERJ solicitamos mais 5 APs com licenciamento que deve ter total compatibilidade com o modelo atual (AP200) e com o modelo do firewall, além de 3 anos de garantia. E para o modelo já existente faremos a extensão de garantia deste item com o objetivo de promover a continuidade do investimento já realizado anteriormente necessário para manter os atuais níveis de disponibilidade da rede Wi-fi corporativa do Conselho Regional de Medicina do Estado do Rio de Janeiro mitigando os possíveis riscos de indisponibilidade dos equipamentos por falha de hardware ou software. Desta forma torna-se essencial a aquisição da extensão da garantia, visando preservar o recurso fornecendo solução de acesso a rede sem fio de forma segura mantendo o padrão de qualidade ofertado ao publico externo indo ao encontro dos objetivos estratégicos do CREMERJ no que tange a segurança da informação.

1.20. A atualização tecnológica do produto na modalidade Trade Up mantendo uma solução de segurança sólida com custo de renovação provendo uma série de vantagens ao CREMERJ tais como:

a) Manter parte do investimento inicial que foi efetuado, uma vez que a solução de segurança de borda é controladora dos pontos de rede sem fio, que em caso de troca teriam de ser trocados/descartados;

b) O impacto no ambiente de produção é mínimo, uma vez que todas as configurações que estão hoje em funcionamento seriam migradas para a nova ferramenta e apenas novos recursos disponibilizados pelo fabricante precisariam efetivamente ser configurados;

c) A não necessidade de investimento em uma nova implementação de produto, bem como capacitação da equipe de TI do CREMERJ para suportar o mesmo.

ESPECIFICAÇÃO DO OBJETO/SERVIÇO

Contratação em lote único de serviço para aquisição de solução de segurança da rede de dados do Conselho Regional de Medicina do Estado do Rio de Janeiro, composta por elementos de hardware e software, incluindo licenciamento, instalação, garantia e suporte técnico. O objeto descrito está subdividido em itens, conforme tabela abaixo, e será adjudicado em nome de uma única empresa.

ITEM	ESPECIFICAÇÃO	QTDE
1	WatchGuard Firebox M570 Series Hardware - PN WGFBM570HW	01 (Um)
2	Trade Up to WatchGuard Firebox M570 with 3-yr Total Security Suite (Software Only) - PN WGTM570MD3TU	01 (Um)
3	WatchGuard Firebox AP320 Hardware - PN WGAP320HW	05 (Cinco)
4	WatchGuard AP320 and 3-yr Standard Support - PN WGLAP320MD3	05 (Cinco)
5	WatchGuard AP200 1-yr LiveSecurity Renewal PN WG019818	07 (Sete)
6	Instalação física e Configuração • Instalação física de todos os equipamentos; • Atualização de Firmware da Solução de Segurança de todos os equipamentos; • Configuração de ambiente de segurança aderente às políticas do cliente de todos os hardwares; • Configuração de Servidor de Relatórios; • Passagem de conhecimento para a equipe; • Documentação;	01 (Um)

Item 1: WatchGuard Firebox M570 Series Hardware - PN WGFBM570HW

1.1. SOBRE A SOLUÇÃO

1.1.1. Solução de segurança (appliance) Firewall – A **CONTRATADA** deverá implantar, fornecer, documentar, treinar e configurar uma solução de segurança baseada em solução de firewall do tipo appliance e demais ferramentas necessárias para promover a segurança da rede do **CONTRATANTE**, incluindo serviços de instalação, configuração de acordo com as necessidades do Conselho, suporte técnico e treinamento;

1.1.2. A **CONTRATANTE** pretende com esta contratação atender a necessidade de aquisição de um sistema de proteção de rede ininterruptamente ativo e de alta disponibilidade, com a adequação de suas funcionalidades, fazendo frente ao crescente número de acessos e novos tipos de ataques, através da implementação de um esquema de alta disponibilidade do produto de Firewall para as conexões recebidas, estabelecimento e otimização de conexões VPN.

1.1.3. A solução de Firewall deverá possibilitar monitorar e controlar o tráfego de dados que circula entre a rede local e a Internet, estabelecendo um único canal de entrada e saída entre aqueles ambientes, permitindo a proteção da rede local (Intranet) contra ações de cracker e hackers.

1.1.4. A solução deverá prover proteção integrada de antivírus, Anti-Spyware, AntiSpam, Anti-Adware, Anti-Keylogger, filtro de conteúdo Web (Proxy) e controle inteligente de aplicações web;

1.1.5. Os equipamentos eletroeletrônicos devem aceitar tensão elétrica de entrada 110V, ou bivolt e atender a norma NBR 14136;

1.2. SOBRE OS EQUIPAMENTOS

1.2.1. Todos os equipamentos e respectivos acessórios e cabeamento especificados neste edital deverão ser novos, estarem em linha de produção do Fabricante e em perfeitas condições para sua instalação e operação imediata. **Não serão aceitos produtos e equipamentos descontinuados pelos seus respectivos Fabricantes**. Todos os equipamentos devem ser do mesmo Fabricante não sendo aceito nenhum tipo de garantia solidária.

1.2.2. Deverão ser entregues em embalagem individual lacrada, adequadamente protegida para transporte do mesmo com segurança.

1.2.3. Os equipamentos e respectivos acessórios deverão estar em conformidade com a presente especificação técnica do produto.

1.2.4. O equipamento a ser descrito tem a finalidade de atender o projeto de Tecnologia da Informação da **CONTRATANTE**, no quesito "Segurança e Gerência de Rede", possibilitando o eficaz gerenciamento e controle dos links de Internet, gerenciamento, estabelecimento e otimização de conexões VPN, gerenciamento unificado de ameaças combinadas com prevenção de intrusão, antivírus, anti-spyware, AntiSpam e filtro de conteúdo web integradas.

1.2.5. Além dos equipamentos e especificações técnicas da Solução de Segurança descritas a seguir, é de responsabilidade da **CONTRATADA** ofertar e prever contemplação de outros equipamentos, cabos, módulos, conversores, softwares e licenças, hardware e/ou acessórios necessários para atender ao pleno funcionamento e com segurança apropriada para as informações e toda a rede de computadores da **CONTRATANTE** devendo ser descriminado na proposta técnica/preço.

1.3. FUNCIONALIDADES GERAIS

1.3.1. Deve suportar três zonas de segurança (redes): externa, privada e opcional (DMZ mínimo de 5).

1.3.2. Deve suportar endereços IP estáticos e dinâmicos (DHCP e PPPoE) na interface externa.

1.3.3. O equipamento de firewall deve permitir DHCPv6 em interfaces externas.

1.3.4. O equipamento de firewall deve possuir um throughput de 8Gbps para firewall e 1.7Gbps para UTM (combinando GAV e IPS).

1.3.5. O equipamento de firewall deve suportar 9.200.000 conexões simultâneas.

1.3.6. O equipamento de firewall deve possuir funcionalidades de UTM, incorporando as funcionalidades de filtro de URL, IPS, GAV, Controle de Aplicação, DLP e proteção contra ameaças day-zero.

1.3.7. O equipamento de firewall deve possuir funcionalidades de um NgFW, incorporando as funcionalidades de filtro de URL, IPS, GAV, Controle de Aplicação, DLP e proteção contra ameaças day-zero.

1.3.8. O equipamento de Firewall deve suportar a implementação de políticas de segurança de camada de aplicação.

1.3.9. Deve suportar em suas políticas de segurança em camada de aplicação (proxies) pré-configurados suportar os seguintes protocolos comuns: HTTP, HTTPS, POP3, SMTP, FTP, DNS, SIP, H323, TCP-UDP, TFTP.

1.3.10. O equipamento de firewall deve suportar autenticação via RADIUS, Secure ID, LDAP e Active Directory.

1.3.11. O equipamento de firewall deve suportar autenticação transparente de usuários de AD (Single SignOn).

1.3.12. O equipamento de firewall deve permitir habilitar e desabilitar SSLv3 em proxies de HTTPS/SMTP.

1.3.13. O equipamento de firewall deve suportar a configuração de regras de proxy explicito para aceitar solicitações de clientes e buscar informação em nome dos clientes.

1.3.14. O equipamento de firewall deve suportar a habilidade de web FTP por proxy explicito para utilizar comandos FTP nativos e enviar dados no formato HTTP response.

1.3.15. O equipamento de firewall deve suportar a habilidade de configurar um proxy SMTP para analisar documentos com macros embutidas e o equipamento também deve possuir uma opção para remover estes macros antes de enviar o documento para seus destinatários.

1.3.16. O equipamento de firewall deve possuir certificados digitais do tipo self-signed para executar deepinspection de pacotes via proxy SMTP sobre TLS.

1.3.17. O equipamento de firewall deve executar deepcontente inspection de dados em proxy HTTPS.

1.3.18. O equipamento de firewall deve limitar o acesso de usuários a site não permitidos pela política de segurança do CREMERJ.

1.3.19. O equipamento de firewall deve definir o intervalo de tempo entre tentativas de login incorretas por conexão FTP em clientes FTP e Server Proxy Actions.

1.3.20. O equipamento de firewall deve possuir a funcionalidade de NTP server e possuir uma política criada automaticamente de NTP para equipamentos conectados em sua rede interna.

1.3.21. O equipamento de firewall deve suportar DNS dinâmico.

1.3.22. O equipamento de firewall deve possuir defesas contra ataques fragmentados, permitindo que o firewall monte os pacotes fragmentados antes de encaminhá-los a redes internas.

1.3.23. O equipamento de firewall deve conseguir filtrar conteúdo nos protocolos mais comuns, assim como filtrar conteúdo tipo “MIME”.

1.3.24. O equipamento de firewall deve proteger e-mails internos contra open relay. Ele deve ser capaz e ser configurado para domínios de e-mail aceitos no ambiente.

1.3.25. O equipamento de firewall deve permitir a configuração de limites para detecção de ataques de flood e Denial of Service (DoS) além de distributed denial of service (DDoS).

1.3.26. O equipamento de firewall deve suportar Protocol Anomaly Detection (PAD) para DNS e outros tipos de protocolos.

1.3.27. O equipamento de firewall deve suportar Server Name Indication (SNI) para configurar domínios para funcionalidades de bloqueio, inspeção ou permissão.

1.3.28. O equipamento de firewall deve complementar capacidades e bloqueio de CN existentes com a finalidade de bloquear domínios específicos do Google.

1.3.29. O equipamento de firewall deve suportar bloqueio e gerenciamento de trafego por domínios especificados por FQDNs (FullyQualified Domain Names) a fim de bloquear sites disponibilizados por Content Delivery Networks (CDNs)

1.3.30. O equipamento de firewall deve suportar o bloqueio de domínios com configurações “wildcard”.

1.4. REQUISITOS VPN

1.4.1. A solução de UTM deve suportar VPN Mobile.

1.4.2. A solução de UTM deve suportar pelo menos 500VPNs Mobile usando IPSec.

1.4.3. A solução de UTM deve suportar ao menos 500 usuários mobile usando VPN SSL.

1.4.4. A solução de UTM deve permitir o download do cliente de VPN SSL através do próprio firewall.

1.4.5. A solução de UTM deve prover clientes SSL para Windows Vista, 7, 8, 10, MAC OS, Android e IOS.

1.4.6. A solução de UTM deve suportar VPN entre localidades (site-to-site VPN).

1.4.7. A solução de UTM deve suportar pelo menos 500VPNs entre escritórios utilizando IPSec.

1.4.8. A solução de UTM deve suportar iterações com outros produtos e marcas que suportam o padrão IPSec.

1.4.9. A solução de UTM deve suportar os seguintes métodos de autenticação: DES, 3DES, AES-128, AES-192, AES-256.

1.4.10. A solução UTM deve suportar os seguintes métodos de criptografia: SHA-2, MD5, IKE Pre-Shared Key, 3rd PartyCert.

1.4.11. A solução de UTM deve suportar DeadPeerDetection (DPD).

1.4.12. A solução de UTM deve suportar IKEv2

1.4.13. A solução de UTM deve suportar Perfect Forward Secrecy (PFS) com chaves Diffie-Hellman (ou Diffie-Hellman-Merkle) em pacotes web e email.

1.4.14. A solução de UTM deve suportar VPN Failover (reestabelecer a VPN através de um segundo link em caso de falha do link primário).

1.4.15. A solução de UTM deve suportar VPN IPSEC com um throughput igual ou maior que 5.3 Gbps

1.4.16. A solução de UTM deve permitir criar interfaces virtuais para VPNs e rotear tráfego utilizando VPNs site-to-site com protocolos de roteamento dinâmico.

1.4.17. A solução de UTM deve suportar Branch Office VPN (BOVPN) de forma que uma interface virtual suporte qualquer interface como gateway local.

1.4.18. A solução de UTM deve suportar configuração de relatórios BOVPN que facilitem o troubleshooting.

1.4.19. A solução de UTM deve permitir visualizar estatísticas de VPN em interfaces virtuais, gateways, tunnel types, etc. para usuários mobile ou não.

1.4.20. A solução de UTM deve permitir visualizar mensagens de diagnóstico de VPN para ajudar a remediar e realizar o troubleshooting pelos administradores do sistema.

1.4.21. A solução de UTM deve suportar single-signon (SSO) em conexões de rede via tuneis BOVPN.

1.4.22. A solução de UTM deve suportar tuneis VPN site-to-site estáticos (políticas) e dinâmicas (roteadas) para soluções em nuvem.

1.5. FILTRAGEM DE CONTEÚDO

1.5.1. A solução de UTM deve suportar filtro de conteúdo via subscrição adicional.

1.5.2. A solução deve permitir que o filtro trabalhe por categorias, ajustado por grupos de usuário e possuir um mínimo de 120 categorias.

1.5.3. A solução de UTM deve permitir exceções no filtro de conteúdo por meio de whitelist.

1.5.4. A solução de UTM deve suportar uma base de dados localizada na nuvem e atualizada dinamicamente.

1.5.5. A solução de UTM deve filtrar conteúdo em múltiplas línguas, incluindo, mas não limitado a: português, inglês, alemão, espanhol, francês, italiano, holandês, japonês, chinês tradicional e simplificado.

1.5.6. A solução de UTM deve limitar o acesso de usuários a sites não permitidos pela política de segurança do CREMERJ.

1.6. LISTA DE BLACKLIST IPS

1.6.1. A solução de UTM deve suportar bloqueio de trafego vindo de IPs maliciosos reconhecidos por base de dados de blackslists disponíveis no mercado.

1.6.2. A solução de UTM deve suportar o bloqueio de trafego de botnets reconhecidos por base de dados de blacklist disponíveis no mercado.

1.7. CONTROLE DE APLICAÇÃO

1.7.1. A solução de UTM deve suportar a filtro de aplicação no próprio hardware UTM através de subscrição adicional.

1.7.2. A solução de UTM deve suportar a configuração de exceções para filtro de aplicação.

1.7.3. A solução de UTM deve ter suas assinaturas de aplicação atualizadas automaticamente e regularmente.

1.7.4. A solução de UTM deve identificar e bloquear mais de 1800 aplicações diferentes, incluindo controle granular de aplicação, como telas de login e metodologias específicas de transferência de arquivo.

1.7.5. A solução de UTM deve suportar updates automáticos de assinaturas de aplicação.

1.7.6. A solução de UTM deve updates de assinatura de aplicação em modo off-line.

1.8. REQUISITOS ANTIVÍRUS

1.8.1. A solução de UTM deve suportar a funcionalidade de antivírus de borda fornecida por fabricantes líderes no segmento de antivírus no mesmo equipamento UTM através de subscrição adicional.

1.8.2. A solução de UTM deve receber atualizações de assinaturas de antivírus automaticamente.

1.8.3. A solução de UTM deve suportar a opção de quarentena para e-mails recebidos.

1.8.4. A solução de UTM deve suportar whitelists para e-mails a fim de receber mensagens de domínios confiáveis em seu ambiente.

1.8.5. A solução de UTM deve ter a capacidade de detectar e bloquear spyware.

1.8.6. A solução de UTM deve ter a capacidade de detectar e bloquear vírus do tipo ransom.

1.8.7. A solução de UTM deve escanear todos os arquivos transferidos mesmo que os mesmos estejam dentro de diversos níveis de compressão (.zip, .tar, .rar, .gzip ou outras extensões de arquivos oriundos de outros compactadores).

1.8.8. A solução de UTM deve suportar os seguintes protocolos: HTTP, FTP, SMTP, POP3.

1.8.9. A solução de UTM deve suportar notas de reputação (1 a 100) para permitir o by-pass de escaneamento de URLs a fim de aumentar a performance da solução.

1.8.10. A solução de UTM deve bloquear automaticamente websites de reputação baixa (histórico de vírus, spam e outros tipos de malware) baseado em informações recebidas por um serviço disponível em nuvem.

1.8.11. A solução de UTM deve suportar um throughput de AntiVirus Gateway de pelo menos 3.2Gbps.

1.8.12. A solução de UTM deve suportar acesso a atualizações de assinaturas automaticamente, manualmente e de forma off-line.

1.9. REQUISITOS ANTISPAM

1.9.1. A solução de UTM deve possuir a funcionalidade de anti-spam através de subscrição adicional dentro do mesmo hardware UTM.

1.9.2. A solução de UTM deve permitir que seu anti-spam deve ser baseada na tecnologia RPD (Recurrent Pattern Detection).

1.9.3. A solução de UTM deve permitir que seu anti-spam deve prover capacidade de quarentena.

1.9.4. A solução de UTM deve permitir que seu anti-spam seja integrado com analise de antivírus spam (detecção de vírus outbreaks).

1.9.5. A solução de UTM deve suportar múltiplas línguas em seu spam-blocker.

1.9.6. A solução de UTM deve bloquear spam baseado em imagens e não apenas texto.

1.10. REQUISITOS IPS – INTRUSION PREVENT SYSTEM

1.10.1. A solução de UTM deve suportar a funcionalidade de IPS no mesmo equipamento via subscrição adicional.

1.10.2. A solução de UTM deve suportar atualizações automáticas de assinaturas de IPS.

1.10.3. A solução de UTM deve permitir que a solução de IPS realize analise em L7 (camada OSI 7) e defina o nível de severidade do ataque, gerando alarmos remotos e notificações de acordo.

1.10.4. A solução de UTM deve suportar bloqueio automático de fontes conhecidas de ataque.

1.10.5. A solução de UTM deve suportar os protocolos mais utilizados como HTTP, FTP, SMTP e POP3.

1.10.6. A solução de UTM deve suportar um throughput de IPS de pelo menos 5.5 Gbps.

1.10.7. A solução de UTM deve permitir o update manual e offline de assinaturas de IPS.

1.11. DATA LOSS PREVENTION

1.11.1. A solução de UTM deve proteger o ambiente contra perda de dados confidenciais (DLP) através de subscrição adicional.

1.11.2. A solução de UTM deve estar em compliance com as iniciativas de PCI e HIPAA.

1.11.3. A solução de UTM deve suportar regras predeterminadas de DLP a fim de identificar dados de cartão de credito, endereços e dados referentes a saúde e números de identificação pessoal.

1.11.4. A solução de UTM deve prever regras predeterminadas para ao mínimo 20 países diferentes.

1.11.5. A solução de UTM deve atualizar assinaturas de DLP (Data LossPrevention) de forma automática, online e manual, offline.

1.12. ADVANCED MALWARE DETECTION / ZERO DAY PREVENTION

1.12.1. A solução de UTM deve suportar a funcionalidade de detecção de malwares avançados no mesmo equipamento através de uma subscrição adicional.

1.12.2. A solução de UTM deve possuir um sistema completo de emulação para detecção de malware durante a o runtime da solicitação e, uma sandbox disponível em nuvem.

1.12.3. A solução de APT do UTM deve suportar todos os arquivos executáveis em Windows como: zip, PDF, Microsoft Office object, e arquivos Android APK.

1.12.4. A solução de UTM deve prover relatórios detalhes com analise identificando o arquivo como malware.

1.13. NETWORK DISCOVERY

1.13.1. A solução de UTM deve permitir aos administradores do firewall a enviarem pacotes UDP para escanear endpoints na rede.

1.13.2. A solução de UTM deve escanear os equipamentos conectados ao firewall, informar suas portas, endereço IP, endereço MAC, hostname, serviços e versão de sistema operacional.

1.13.3. A solução de escaneamento de rede deve possibilitar a detecção de equipamentos aprovados e rogue na rede.

1.14. MOBILE SECURITY

1.14.1. A solução de UTM deve permitir a configuração de requisitos mínimos para equipamentos iOS e Android para que estes trafeguem na rede.

1.14.2. A solução de UTM deve permitir o monitoramento e exigir que as configurações destes equipamentos móveis estejam em compliance com relação a versões de OS aprovadas, verificar se o hardware está rooted ou jaibroken além de escanear malware e adware em aparelhos Android.

1.14.3. A solução de UTM deve fornecer um dashboard consolidado para verificação de compliance dos dispositivos móveis.

1.14.4. A solução de UTM deve utilizar a funcionalidade de DHCP fingerprinting para determinar o tipo de dispositivo conectado na rede.

1.14.5 A solução de UTM deve ter compatibilidade ao modelo de Acess Point WatchGuard AP200.

1.15. NETWORK CAPABILITIES

1.15.1. O equipamento deve fornecer no mínimo as seguintes interfaces: 6x 10/100/1000BaseT e duas portas SFP 10/100/1000; Estas interfaces deve ser configuráveis como qualquer uma das três zonas de segurança informados no **item 3.1.1.1.**

1.15.2. O firewall deve suportar transceivers opticos que devem estar inclusos para todas as portas de fibra optica do produto.

1.15.3. O firewall deve suportar configuração de multi-wan, permitindo um mínimo de 04 conexões externas para a internet.

1.15.4. As interfaces do firewall devem suportar operação em modo fail-over.

1.15.5. As interfaces externas do firewall devem ser capazes de operar em modo round-robin com pesos customizáveis.

1.15.6. As interfaces externas do firewall devem ser capazes de operar em modo overflow, permitindo o uso de links externos quando a capacidade do link principal for excedia.

1.15.7. O equipamento de firewall deve suportar um mínimo de 500 VLANs.

1.15.8. O equipamento de firewall deve prover controle de banda definido por política, protocolo e grupo de usuários.

1.15.9. O equipamento de firewall deve possuir controle de banda por interface.

1.15.10. O equipamento de firewall deve possuir controle de banda por endereço IP e VLAN.

1.15.11. O equipamento de firewall deve permitir a configuração de cotas por tempo e tráfego por usuário, podendo notificar o mesmo em caso de atingimento da cota estabelecida.

1.15.12. O equipamento de firewall deve suportar configuração em modo router (routing), drop-in (mesmo IP em todas suas interfaces) e em modo transparent bridge.

1.15.13. O equipamento de firewall deve suportar NAT estático, NAT dinâmico e 1-1 NAT.

1.15.14. O equipamento de firewall deve suportar alta disponibilidade em modo ativo-passivo e ativo-ativo.

1.15.15. O equipamento de firewall deve suportar policy-basedrouting (PBR), permitindo que os administradores especifiquem parâmetros para definir por qual interface externa o trafego da rede será enviado.

1.15.16. O equipamento de firewall deve suportar NAT e PAT.

1.15.17. O equipamento de firewall deve suportar Server LoadBalancing para servidores internos.

1.15.18. O equipamento de firewall deve suportar NAT estático (Portforwarding).

1.15.19. O equipamento de firewall deve suportar NAT dinâmico.

1.15.20. O equipamento de firewall deve permitir a implementação de NAT 1-1.

1.15.21. O equipamento de firewall deve suportar NAT Traversal para IPSEC.

1.15.22. O equipamento de firewall deve suportar policy-based NAT.

1.16. GESTÃO DA SOLUÇÃO

1.16.1. A solução de UTM deve prover administração em tempo real do equipamento via gerenciamento por interface gráfica.

1.16.2. A solução de UTM deve suportar o monitoramento em tempo real de logs gerados pelo equipamento.

1.16.3. A solução de UTM deve suportar o envio de diversos tipos de alerta através de SNMP ou e-mail.

1.16.4. A solução de UTM suporta o uso de NAT para conexões via SNMP application layer gateway.

1.16.5. A solução de UTM deve suportar gerência através de múltiplos computadores simultaneamente.

1.16.6. A solução de UTM deve suportar VPN entre equipamentos, configurável via drag-and-drop.

1.16.7. A solução de UTM deve permitir a criação de templates de configuração VPN hub-and-spoke.

1.16.8. A solução de UTM deve suportar funcionalidade de “rollback” para configurações prévias.

1.16.9. A solução de UTM deve suportar o protocolo de gerenciamento DVCP.

1.16.10. A solução de UTM deve suportar a edição de políticas de segurança de modo offline ou em GUI.

1.16.11. A solução de UTM deve permitir a edição de políticas através de Windows GUI e interface CLI.

1.16.12. A solução de UTM deve suportar diferentes níveis de administradores com acessos distintos.

1.16.13. A solução de UTM deve suportar autenticação com Windows Active Directory.

1.16.14. A solução de UTM deve suportar a gerência via web browser.

1.16.15. A solução de UTM deve suportar login via SSO (single-signon) para RDP.

1.16.16. A solução de UTM deve suportar MS Exchange Server 2013 para SSO Exchange Monitor.

1.16.17. A solução de UTM deve suportar a troca de múltiplos usuários utilizando um cliente SSO instalado em Windows Vista, Windows 7, Windows 8, Server 2008, Server 2012, Server 2016.

1.16.18. A solução de UTM deve suportar equipamentos que são gerenciados via linha de comando, porta serial ou SSH.

1.16.19. A solução de UTM deve suportar interface de usuário via web para gerência do equipamento, devendo ser compatível com tablets e outros equipamentos móveis.

1.16.20. A solução de UTM deve suportar o rastreamento de configuração e deve permitir a indicação das diferenças entre duas configurações salvas em datas diferentes.

1.16.21. A solução de UTM deve suportar a criação de arquivos de configuração offline sem estar diretamente conectado ao firewall.

1.16.22. A solução de UTM deve suportar a instalação em ambientes remotos sem a necessidade de funcionário com conhecimento técnico on-site. O produto deve possuir capacidade de baixar uma configuração armazenada na nuvem quando o equipamento for iniciado pela primeira vez.

1.16.23. A solução de UTM deve permitir a mudança da interface externa por meio de um arquivo CSV.

1.16.24. A solução de UTM deve suportar SSO para Radius em um servidor fornecido separadamente.

1.16.25. A solução de UTM deve rastrear a sessões de usuário através da funcionalidade de SSO Radius.

1.16.26. A solução de UTM deve destacar as diferenças entre versões de configuração do firewall.

1.17. LOGS E RELATÓRIOS

1.17.1. A solução de UTM deve permitir a implementação de servidores externos de maneira que todos os logs e relatórios sejam armazenados de forma centralizada.

1.17.2. A solução de UTM não deve ter custos adicionais para armazenamento e criação de logs e relatórios.

1.17.3. A solução de UTM deve suportar TCP (Transport Control Protocol) e utilizar uma base de dados SQL para garantir escalabilidade.

1.17.4. A solução de UTM deve suportar o envio de LOGs simultaneamente e múltiplos servidores de log.

1.17.5. A solução de UTM deve permitir a configuração de servidores de LOG backup, que serão utilizados caso o servidor primário apresente falhas.

1.17.6. A solução de UTM deve criptografar a transmissão de logs dos firewall para seu envio ao servidor sem a necessidade de VPN.

1.17.7. A solução de UTM deve possuir mais de 90 relatórios predefinidos sem qualquer custo extra ou adicional.

1.17.8. A solução de UTM deve alertar o administrador da rede quando a base de dados de log e relatórios atingir um valor próximo ao seu limite estipulado.

1.17.9. A solução de UTM deve suportar a extração de relatórios nos formatos PDF e CSV.

1.17.10. A solução de UTM deve possuir relatórios de compliance para HIPAA e PCI.

1.17.11. A solução de UTM deve elaborar relatórios automaticamente assim como seu envio por e-mail.

1.17.12. A solução de UTM deve possuir um relatório executivo com informações de “High Level”.

1.17.13. A solução de UTM deve permitir a execução de pivot e drilldown em informações mais detalhadas a partir de qualquer item logado.

1.17.14. A solução de UTM deve suportar o envio automático de todos os tipos de relatórios por e-mail.

1.17.15. A solução de UTM deve suportar controle de acesso por usuário com a finalidade de garantir o devido acesso e ações tomadas por usuário.

1.17.16. A solução de UTM deve possuir imagens virtuais da solução de relatório e armazenamento de logs.

1.17.17. A solução de armazenamento de logs e relatórios deve ser compatível com VMware.

1.17.18. A solução de UTM deve possuir uma visão tipo “treemap” para indicar o tipo de trafego passando pelo equipamento de forma gráfica.

1.17.19. A solução de UTM deve suportar uma solução de visibilidade de demonstre em um mapa mundi a origem e destino de trafego de aplicações, trafego negado, e eventos de IPS.

1.17.20. A solução de UTM deve suportar relatórios de IPS que indiquem informações detalhadas e referencias CVE para cada evento alertado.

1.17.21. A solução de UTM deve permitir agregar diversos firewalls em forma de grupos.

1.17.22. A solução de UTM deve suportar o log de Single SignOn (SSO) para melhorar a monitoria.

1.17.23. A solução de UTM deve suportar o monitoramento de logs de loadbalancing e de eventos instalados em múltiplos domínios.

1.17.24. A solução de UTM deve suportar um agente SSO que envie uma resolução de DNS para resolver o nome do host para aquele endereço IP e determinar em qual domínio o cliente pertence.

1.17.25. A solução de visibilidade deve suportar visibilidade por FQDN em forma de relatório através do equipamento de firewall.

1.17.26. A solução de visibilidade deve demonstrar o volume de banda e tempo utilizado por usuário em forma de relatório acessível através do equipamento ou via web UI.

1.17.27. A solução de visibilidade deve possuir um dashboard com a habilidade de bloquear a origem de um ataque por IP diretamente pelo painel.

1.17.28. A solução de UTM deve permitir que o painel de visibilidade tenha funções para criação de políticas de firewall.

1.17.29. A solução de UTM deve possuir um relatório indicando o uso de cada política, inclusive as políticas não utilizadas no firewall.

1.17.30. A solução de UTM deve possuir um painel de visualização que efetivamente demonstre, de forma geográfica, o destino de trafego que passa pelo firewall e as políticas que foram acionadas.

Item 2: Trade Up to WatchGuard Firebox M570 with 3-yr Total Security Suite (Software Only) - PN WGTM570MD3TU

A rede precisa de mecanismos de varredura para se proteger contra sypware, vírus, aplicativos maliciosos e vazamento de dados incluindo ramsomware, botnets, ameaças persistentes avançadas e malware. A solução de rede lidará com todos os aspectos de prevenção de ameaça, detecção, correlação e resposta o quanto antes à medida que essas ameaças evoluem, incluindo, sem limitação a prevenção e resposta imediata contra ransomware e malwares avançados. O Total Security Suite possui além da proteção de malware avançada, proteção contra perda de dados, recursos aprimorados de visibilidade de rede e a capacidade de agir contra ameaças diretamente na plataforma. Também deve incluir suporte de nível de *Gold* 24x7. Além disso, todos os serviços tradicionais de segurança de rede típicos de um *appliance* UTM devem estar presentes: IPS, GAV, filtragem de URL, controle de aplicativos, bloqueio de spam e pesquisa de reputação.

2.1. ESPECIFICAÇÃO DO TOTAL SECURITY SUITE

2.1.1. SERVIÇOS DE SEGURANÇA INCLUSOS NO TOTAL SECURITY SUITE

2.1.1.1. SERVIÇO DE PREVENÇÃO DE INTRUSÕES (IPS)

O IPS usa assinaturas atualizadas continuamente para varrer o tráfego na maioria dos protocolos para fornecer proteção em tempo real contra ameaças, incluindo spyware, injeções de SQL, script entre sites e estouro de buffer.

2.1.1.2. SERVIÇO REPUTATIONENABLED DEFENSE (RED)

Um serviço de busca de reputação baseado em nuvem que protege os usuários da web de sites e botnets maliciosos, aprimorando drasticamente o processamento de web.

2.1.1.3. FILTRAGEM DE URLWEBBLOCKER

Além de bloquear automaticamente sites maliciosos conhecidos, o conteúdo granular do WebBlocker e as ferramentas de filtragem de URL permitem que você bloqueie conteúdos inadequados, conserve a largura de banda da rede e aumente a produtividade dos funcionários.

2.1.1.4. SPAMBLOCKER

Detecção de spam em tempo real para proteção contra surtos. O spam Blocker é tão rápido e eficaz que consegue analisar até 4 bilhões de mensagens por dia.

2.1.1.5. ANTIVÍRUS DO GATEWAY (GAV)

Avalie nossas assinaturas atualizadas continuamente para identificar e bloquear spywares, vírus, cavalos de troia, rogueware e ameaças combinadas conhecidos, incluindo as novas variantes dos vírus conhecidos. Ao mesmo tempo, a análise heurística rastreia dados, construções e ações suspeitos para garantir que os vírus desconhecidos não passem despercebidos.

2.1.1.6. CONTROLE DE APLICATIVOS

Permita, bloqueie ou restrinja o acesso a aplicativos de forma seletiva com base no departamento do usuário, função e horário do dia e veja, em tempo real, o que está sendo acessado na sua rede e por quem.

2.1.1.7. PREVENÇÃO DE PERDADE DADOS (DLP)
Este serviço impede perda de dados maliciosa ou acidental verificando textos e tipos de arquivo comuns para detectar informações confidenciais que tentam sair da rede.

2.1.1.8. APT BLOCKER – PROTEÇÃO AVANÇADA CONTRA MALWARE

O APT Blocker usa uma simulação de última geração para detectar e impedir a maioria dos ataques sofisticados, incluindo ransomware, ameaça de primeiro dia e outros malwares avançados.

2.1.1.9. DIMENSION COMMAND

O Dimension traduz os dados coletados de todos os dispositivos na rede em inteligência acionável sobre a rede e as ameaças. O Dimension Command fornece a capacidade de tomar uma medida para aliviar essas ameaças instantaneamente de um console central.

2.1.1.10. DESCOBERTA DE REDE

Um serviço baseado em assinatura para os dispositivos Firebox que gera um mapa visual de todos os nós na sua rede para que seja possível ver com facilidade onde há riscos presentes.

2.1.1.11. THREAT DETECTION AND RESPONSE

Correlacione eventos de segurança de terminal e rede com inteligência contra ameaças de grau empresarial para detectar, priorizar e ativar a ação imediata para impedir ataques de malware, evoluindo o modelo existente para estender a prevenção passada incluindo correlação, detecção e resposta.

2.1.1.12. SUPORTE

O suporte deve ser prestado dentro das 24 (vinte e quatro) horas do dia pelos 7 (sete) dias da semana.

Item 3: WatchGuard Firebox AP320 Hardware – PN WGAP320HW

3. ESPECIFICAÇÃO TÉCNICA DO *ACCESS POINT* - PONTOS DE ACESSO DE REDE SEM FIO

3.1. Possibilitar operar com modelos de 1 ou 2 rádios;

3.2. Suportar frequências de 2.400-2.474GHz, 5.150-5.250GHz, 5.250-5.350GHz, 5.470-5.725GHz, 5.725-5.850GHz;

3.3. Possuir 6 antenas omnidirecionais;

3.4. Trabalhar com velocidade de dados de 1.3 Gbps para padrão 11ac e de 450 Mbps para padrão 11n;

3.5. Deve suportar temperaturas entre 0 e 40 graus centigrados;

3.6. Possuir energização em PoE 802.3af/at ou Adaptador A/C;

3.7. Suportar no mínimo 16 SSID no mesmo equipamento;

3.8. Suportar os seguintes padrões IEEE: 802.11a/b/g/n/ac, 802.11i, 802.1q, 802.1X, 802.3af/at, 802.11e;

3.9. O gerenciamento da rede sem fio não deve adicionar nenhum equipamento adicional (função controller) na solução oferecida, devendo ser tratado pelo appliance UTM físico ou virtual;

Item 4: WatchGuard AP320 and 3-yr Standard Support - PN WGLAP320MD3

4. Os *Access points* devem ter garantia, atualização e suporte de 36 (trinta e seis) meses.

Item 5: WatchGuard AP200 1-yr LiveSecurity Renewal PN WG019818

5. SERVIÇOS ASSEGURADOS NA EXTENSÃO DA GARANTIA

A extensão de garantia atenderá aos seguintes itens:

- Deve contemplar a substituição do equipamento em caso de problema físico.

- Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:

a. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento;

b. Deve assegurar a utilização de novas/atualizações de versões de software da solução sem ônus a Licitante;

c. Deve permitir o acesso à base de conhecimento da solução;

Item 6: Instalação

ETAPAS DA INSTALAÇÃO:

Item	Descrição
1	Instalação física dos modelos adquiridos: M570, AP320 e remanejamento do AP200 para outros locais
	Configuração do M570
	Configuração e atualização dos APs já existentes na nova solução (Modelo já instalado AP200) e dos AP320.
	Atualização de firmware da solução de segurança
	Configuração de ambiente de segurança aderente às políticas do cliente
	Configuração de servidor de relatórios
	Passagem de conhecimento para a equipe
	Documentação

6. SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA

6.1. Quanto aos serviços:

6.1.1. A **CONTRATADA** deverá preparar, instalar e configurar a solução ofertada, na Sede do CREMERJ.

6.1.2. A instalação da solução de segurança de rede deverá ser feita por profissionais devidamente qualificados e certificados na área de segurança do fabricante.

6.1.3. A prestação dos serviços de instalação e configuração deverá compreender entre outros, os seguintes procedimentos: Análise da topologia e arquitetura da rede da **CONTRATANTE**, considerando os ativos de rede instalados, acesso à Internet, sites remotos (subsedes e seccionais na capital e no interior, CFM (Conselho Federal de Medicina), serviços de rede oferecidos aos usuários internos e externos, regras de firewall existentes, bem como qualquer outro equipamento ou sistema relevante na segurança do perímetro, sendo então feita a configuração da solução de segurança de acordo com as exigências levantadas, visando:

6.1.3.1. Facilitar o gerenciamento e a solução de eventuais problemas, com a proposição de eventuais correções na topologia da rede e implementação de alguns protocolos com a finalidade de minimizar os riscos e aumentar a disponibilidade do sistema.

6.1.3.2. Realizar o projeto de segurança do perímetro, considerando todos os serviços fornecidos aos usuários internos e externos da **CONTRATANTE**.

6.1.3.3. Emissão de relatório, contendo todas as informações coletadas e a sugestão de configuração.

6.1.3.4. Aplicação de todas as funcionalidades definidas no projeto e implantação do gerenciamento da solução.

6.1.3.5. Realização de testes de funcionamento.

6.1.4. Durante toda a implantação do projeto, o técnico da **CONTRATADA** deverá demonstrar à equipe técnica de acompanhamento da **CONTRATANTE** como instalar e configurar a solução e/ou softwares fornecidos (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos entregues.

6.1.5. Todo o processo de instalação e configuração do sistema deverá ser documentado pela **CONTRATADA** sob a forma de relatório ou roteiro, de forma que a equipe técnica da **CONTRATANTE** possa reproduzir a instalação da solução de segurança quando necessário consultando a documentação.

6.1.6. Deverão ser configuradas todas as características disponíveis nos produtos fornecidos e solicitadas pela **CONTRATANTE**.

6.1.7. Todas as configurações de regras, políticas, Black e White list, VPNs implantadas e configuradas no firewall atual deverão ser importadas ou reconfiguradas no novo firewall de forma que os serviços não sejam impactados.

6.1.8. Os Access points existentes devem ser atualizados para ultima versão do firmware e configurado no novo equipamento de firewall mantendo a política atual utilizando as melhores praticas de segurança dentro do novo ambiente.

6.1.9. A instalação e configuração definitivas do software para segurança de rede (entrada definitiva em produção substituindo o sistema existente) poderão ser feitas fora do horário normal de expediente da **CONTRATANTE**, (segunda à sexta de 09:00 às 18:00h), se necessário, a fim de minimizar o impacto da migração nos ambientes de trabalho. Tais atividades ocorrerão sem ônus adicional à **CONTRATANTE**.

6.1.10. Todos os equipamentos deverão passar por testes individualizados e integrados garantindo a correta implementação seguindo todos os *baselines* apresentados pela solução assegurando o nível aceitável de segurança da informação para a organização.

Qualificação técnica

7. QUALIFICAÇÃO TÉCNICA

7.1. Como qualificação técnica, a **CONTRATADA** deverá apresentar juntamente com os documentos de habilitação, a seguinte documentação:

7.1.1. Atestado de capacidade técnica emitida por instituição ou empresa de direito público ou privado no Brasil, impresso em papel timbrado (não serão aceitas declarações genéricas de catálogos, manuais ou Internet), com nome e telefone de contato dos responsáveis pela informação atestada, comprovando que a licitante forneceu solução de características semelhantes ao especificado neste termo de referência, prestando a devida garantia e suporte técnico. O documento deverá ainda atestar a satisfação da instituição ou empresa de direito público ou privado no Brasil com o produto ofertado pela licitante.

Garantia

8. ESPECIFICAÇÃO DA GARANTIA

8.1. A garantia deverá ser de **TRINTA E SEIS (36) meses**.

8.2. Deve contemplar a substituição do equipamento em caso de problema físico.

8.3. Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:

8.3.1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento; Deve assegurar a utilização de novas versões de software da solução sem ônus a **CONTRATANTE.**

8.3.2. Deve permitir o acesso à base de conhecimento da solução;

8.3.3. A **CONTRATADA** deverá garantir junto ao fabricante a prestação de serviços de garantia no termo contratual da solução de segurança de rede, sem ônus adicionais à **CONTRATANTE**, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem, acondicionamento, ou outro qualquer durante o período de operação.

8.3.4. Deverão estar abrangidos pela garantia ainda, os serviços de identificação dos componentes, peças e materiais responsáveis pelo mau funcionamento do sistema.

8.3.5. A garantia deverá ser pelo período de, no mínimo, 36 (trinta e seis) meses a contar da data do TERMO DE RECEBIMENTO DEFINITIVO.

8.3.6. Os serviços de garantia dos equipamentos deverão ser prestados por empresa credenciada pelo fabricante dos produtos fornecidos.

8.3.7 Durante o período de garantia (trinta e seis meses), a **CONTRATADA** deverá garantir junto ao fabricante sem ônus para a **CONTRATANTE**, o fornecimento das atualizações (*patches*) corretivas do software e firmware dos equipamentos fornecidos, bem como o recebimento de atualizações (assinatura) do software da solução de segurança.

8.3.8. A **CONTRATADA** deverá garantir junto ao fabricante a prestação dos serviços de garantia nas seguintes condições:

8.3.8.1. Os serviços serão solicitados à Central de Atendimento indicada pela **CONTRATADA**, por meio de abertura de chamado técnico efetuada por técnicos da **CONTRATANTE**.

8.3.8.2. Os componentes, peças e materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento.

8.3.8.3. Caso o equipamento defeituoso não possa ser consertado no prazo descrito ou deva ser reparado em laboratório, o FABRICANTE deverá providenciar substituição temporária, do equipamento, instalando e configurando outro equipamento idêntico, de forma que não haja interrupção nas atividades dos usuários.

8.3.8.4. A **CONTRATADA** deverá garantir junto ao o FABRICANTE que eventuais reparos em laboratório, o deslocamento de equipamentos e seu retorno ao local de origem serão de responsabilidade do FABRICANTE.

8.3.8.5. Os serviços prestados em garantia, incluindo as substituições de hardware, não terão qualquer ônus adicional para a **CONTRATANTE**.

Prazo para atendimento

9. PRAZO PARA ATENDIMENTO E SOLUÇÃO DE PROBLEMAS REFERENTES À GARANTIA E SUPORTE TÉCNICO

Em caso de problemas detectados nos sistemas ofertados considere-se o seguinte:

▪ Caso haja suspensão total no funcionamento das soluções compostas por essas ferramentas, o atendimento e suporte que a **CONTRATADA** deverá garantir junto ao FABRICANTE deverão obedecer aos seguintes prazos:

a) para o atendimento ao chamado: 2 (duas) horas;

b) para a solução do problema: 6 (seis) horas;

▪ Caso o problema detectado não tenha causado a suspensão total no funcionamento das soluções compostas por essas ferramentas, os prazos serão os que seguem:

a) para o atendimento ao chamado: 2 (duas) horas;

b) para a solução do problema: 24 (vinte e quatro) horas;

10. SERVIÇOS DE SUPORTE TÉCNICO DA SOLUÇÃO DE SEGURANÇA APÓS IMPLEMENTAÇÃO

10.1. A **CONTRATADA** deverá prestar serviços de suporte técnico pelo período mínimo de 90 dias contados a partir da data do TERMO DE RECEBIMENTO DEFINITIVO sem quaisquer ônus adicionais à **CONTRATANTE**, que abrangerá:

i. Auxiliar na análise, utilização e configuração da solução.
ii. Auxiliar na identificação é solução de problemas em software e hardware.
iii. Auxiliar na instalação e configuração de atualizações de firmware e software (patches), bem como de novas versões dos produtos;
iv. Auxiliar na auditoria e análise de logs.
v. Encaminhar, a pedido da **CONTRATANTE** incidentes ao fabricante da solução.
vi. Os serviços serão solicitados à Central de Atendimento indicada pela **CONTRATADA**, por meio de abertura de chamado técnico efetuada por técnicos da **CONTRATANTE**.
vii. Os serviços poderão ser prestados na modalidade de atendimento remoto, por meio de chamados.
viii. Os técnicos da **CONTRATANTE** deverão ter acesso à base de conhecimento dos produtos ofertados, via website do fabricante, visando obter informações sobre a solução de segurança fornecida.
ix. Os serviços de suporte técnico não terão qualquer ônus adicional para a **CONTRATANTE**.

11. CONDIÇÕES DE RECEBIMENTO DAS LICENÇAS E DOS EQUIPAMENTOS

11.1. As licenças e os equipamentos deverão ser entregues em no máximo 15 (quinze) dias, contados a partir do recebimento pela Adjudicatária da convocação expressa encaminhada pela **CONTRATANTE** juntamente com a Nota de Empenho.

12. DA ENTREGA

12.1. A entrega deverá ser na Sede do Conselho Regional de Medicina do Estado do Rio de Janeiro, localizada na Praia de Botafogo, 228 / Lj 119B, Botafogo – Rio de Janeiro, RJ, CEP 22.250-145, no horário de 09:00h às 17:00h.

OBRIGAÇÕES DA CONTRATADA

13. OBRIGAÇÕES DA CONTRATADA

13.1. Cumprir fielmente toda a execução do objeto, de acordo com as condições e exigências previamente estabelecidas;

13.2. Fornecer garantia dos equipamentos durante toda vigência Contratual;

13.3. Fornecer garantia dos hardwares/peças substituídos pelo prazo de 36 (trinta e seis) meses, sem prejuízo da garantia contratual;

13.4. Comunicar à CONTRATANTE qualquer anormalidade que esteja impedindo a execução contratual dos serviços de suporte, prestando os esclarecimentos julgados necessários;

13.5. Responsabilizar-se por todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços fornecidos, bem como pelo custo do frete e outros inerentes à execução do objeto, apresentando os documentos fiscais em conformidade com a legislação vigente;

13.6. Assumir todas as despesas com transporte, hospedagem e outros custos operacionais decorrentes da execução do objeto;

13.7. Responsabilizar-se pela fiel execução contratual, respondendo civil e criminalmente pelos danos diretos, que, por dolo ou culpa sua ou de seus empregados, causarem a CONTRATANTE ou a terceiros, sendo admitido o direito a ampla defesa;

13.8. Prestar serviços de suporte e assistência técnica aos bens pelo período de vigência do contrato, de acordo com a forma e regime estabelecidos;

13.9. Observar rigorosamente todos os prazos de atendimento e resolução de chamados estabelecidos, bem como as datas das visitas preventivas, sob pena de aplicação de multa e demais cominações pelo CREMERJ;

13.10. Agir de forma proativa, objetivando prevenir a ocorrência de erros e defeitos, por meio das inspeções nos equipamentos, componentes, dispositivos e softwares de configuração, bem como a coleta e avaliação de logs, atualização, verificação e inspeção visual das condições de funcionamento dos equipamentos, seus componentes e dispositivos;

13.11. Reparar eventuais falhas apresentadas nos equipamentos, compreendendo serviços de conserto, reparos e/ou substituição de bens, componentes e dispositivos, bem como sua configuração e gerenciamento, com vistas a normalidade da operação dos serviços prestados;

13.12. Utilizar os manuais dos produtos e as diretrizes da TI da CONTRATANTE, para desinstalação, reconfiguração ou reinstalação de hardware e/ou software, atualização de versões de drivers, firmwares e software básico, correção de defeitos técnicos, ajustes e reparos necessários;

13.13. Prover toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas realeases, versions, builds e upgrades às suas expensas;

13.14. Utilizar nos serviços profissionais certificados pelo fabricante dos equipamentos, qualificados e tecnicamente capacitados nos produtos em questão;

13.15. Fornecer a sua equipe técnica todas as documentações, manuais, ferramentas e meios técnicos necessários para a execução do objeto, sem custos adicionais ao CREMERJ;

13.16. Fornecer novas versões e atualizações de firmware dos produtos, se houver, sem custos adicionais ao CREMERJ;

13.17. Trocar peças ou substituir peças/bens sempre que identificado ocorrências técnicas que justifiquem;

13.18. Fornecer peças novas e de primeiro uso, lacradas em sua embalagem original;

13.19. Abster-se de desativar hardware, software ou quaisquer outros recursos computacionais do CREMERJ, sem prévio conhecimento e autorização expressa da Administração;

13.20. Fornecer equipamento de redundância, com características iguais ou superiores, sempre que precisar desativar hardware, software ou quaisquer recursos computacionais do CREMERJ, até que o problema seja sanado;

13.21. Responder e ressarcir ao CREMERJ ou a terceiros por eventuais danos diretos causados, inclusive por seus empregados ou prepostos, na execução dos serviços;

13.22. Responsabilizar-se pelo sigilo e confidencialidade, por si e seus empregados, dos documentos e/ou informações que lhe chegarem ao conhecimento por força da execução do contrato, e tenham sido definidas como confidenciais, não podendo divulgá-lo, sob qualquer pretexto, conforme as diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações do CREMERJ ou por qualquer normatização análoga ou que venha a substituir essa;

13.23. Disponibilizar uma infraestrutura de atendimento via telefone ou web, para recebimento e registro dos chamados técnicos realizados pelo CREMERJ, disponibilizando sempre um número de protocolo para controle de atendimento;

13.24. Entregar ao CREMERJ, às suas expensas, toda documentação técnica (relatórios técnicos) gerada em função da execução do Contrato;

13.25. Velar para que todos os privilégios de acesso a sistemas, dados ou informações do CREMERJ sejam utilizados exclusivamente na execução contratual, e pelo período estritamente essencial à realização de serviços;

13.26. Refazer ou corrigir serviços às suas expensas, no todo ou em parte, sempre que identificado pelo CREMERJ ter sido realizado em desacordo com o estabelecido no Termo de Referência;

13.27. Cumprir o cronograma de visitas programadas (manutenção preventiva) definido pelo CREMERJ;

13.28. Responder pelos danos causados diretamente ao CREMERJ ou a terceiros, decorrentes de sua culpa ou dolo, durante a execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou o acompanhamento pelo CREMERJ;

13.29. Responder por quaisquer danos causados diretamente aos equipamentos, softwares, informações e a outros bens de propriedade do CREMERJ, quando esses tenham sido ocasionados por seus técnicos durante a prestação dos serviços objeto desta contratação.

13.30. Durante o processo de implementação da solução de firewall, update de firmware da solução ofertada ou *access points* existentes testes de conformidade deverão ser executados individualmente visando a aferição da real capacidade técnica bem como a configuração de segurança atendendo as melhores práticas de segurança da informação buscando comprovar juntamente com a documentação do fabricante que os equipamentos de fato atendem aos requisitos constantes da especificação técnica. Nesse sentido, os testes serão efetuados em todos os itens de hardware e software da solução.

Termo de referência elaborado por: Setor de TI - CREMERJ.

ANEXO III - MODELO DA PROPOSTA DE PREÇOS

PROPOSTA DE PREÇOS

Nome da Empresa: _____
CNPJ e Endereço:_____
Telefone:_____ E-mail de contato: _____
Nome do Responsável(is) legal(is) pela assinatura do contrato:_____
Identidade: _____ CPF: _____
Contato: Sr(a). _____ Telefone: _____

OBJETO: Contratação de empresa para aquisição de solução de segurança da rede de dados do Conselho Regional de Medicina do Estado do Rio de Janeiro (CREMERJ), composta por elementos de hardware e software, incluindo licenciamento, instalação, garantia e suporte técnico.

ITEM	OBJETOS	QUANT.	VALOR MÁX. UNIT.	VALOR MÁX. GLOBAL
1	WatchGuard Firebox M570 Series Hardware - PN WGFBM570HW	1 (um)	R$ XXX	R$ XXX
2	Trade Up to WatchGuard Firebox M570 with 3-yr Total Security Suite (Software Only) - PN WGTM570MD3TU	1 (um)	R$ XXX	R$ XXX
3	WatchGuard Firebox AP320 Hardware - PN WGAP320HW	5 (cinco)	R$ XXX	R$ XXX
4	WatchGuard AP320 and 3-yr Standard Support - PN WGLAP320MD3	5 (cinco)	R$ XXX	R$ XXX
5	WatchGuard AP200 1-yr LiveSecurity Renewal PN WG019818	7 (sete)	R$ XXX	R$ XXX
6	- Instalação física e Configuração - Atualização de Firmware da Solução de Segurança - Configuração de ambiente de segurança aderente às políticas do cliente - Configuração de Servidor de Relatórios - Passagem de conhecimento para a equipe - Documentação	1	R$ XXX	R$ XXX
VALOR MÁXIMO GLOBAL = (Soma dos valores dos itens 1 + 2 + 3 + 4 + 5 + 6)				R$ XXX

Validade da Proposta: 60 (sessenta) dias.

Os valores acima englobam todos os serviços, incluindo instalação, garantia, materiais, encargos, frete, tributos ou ainda, despesas de quaisquer outras naturezas para a perfeita execução do contrato e a remuneração da Contratada.

Observações:

1) **Será vencedor** aquele que ofertar o MENOR VALOR GLOBAL, ou seja, aquele licitante que apresentar o menor valor quanto a soma dos Itens 1, 2, 3, 4, 5 e 6;

2) **Serão desclassificadas as propostas**: a) que apresentarem valor unitário para os Itens 1, 2, 3, 4, 5 e 6 e valor global superiores ao indicado na *Cláusula 7.1 do Edital.*

ANEXO IV - MINUTA DE CONTRATO

PROCESSO n. 039/2017
PREGÃO n. 001/2018
CONTRATO n. XXX/XX

CONTRATO DE PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO DE JANEIRO – CREMERJ E A EMPRESA _____

Aos ____dias do mês de _____do ano de 2018, presente de um lado, o **CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO DE JANEIRO - CREMERJ,** CNPJ n.º 31.027.527/0001-33, situado na Praia de Botafogo, n.º 228/loja 119-B, Botafogo, Rio de Janeiro/RJ, neste ato representado pelo seu Diretor-Presidente, **Dr. Nelson Nahon**, portador da carteira de identidade nº ******* emitida pelo CREMERJ e CPF nº **********, adiante denominado apenas **CONTRATANTE** e, de outro lado, a empresa _____, portadora do CNPJ n.º _____, Inscrição Estadual n.º _____, com sede na _____, neste ato representada por seu representante legal, Sr./Sra. _____, inscrito (a) no CPF/MF sob o número _____ e portador (a) da carteira de identidade n.° _____ a seguir designada simplesmente **CONTRATADA**, resolveram firmar o presente Contrato de prestação de serviços, tudo mediante as seguintes cláusulas e condições.

CLÁUSULA PRIMEIRA – DAS REGRAS APLICÁVEIS

1.1. O presente Contrato rege-se pelas disposições da Lei 8.666 de 21.06.93, suas alterações e demais disposições legais em vigor ou que venham a disciplinar as licitações e os contratos no âmbito da Administração Pública Federal e às disposições do procedimento licitatório que ensejaram a presente contratação.

CLÁUSULA SEGUNDA - DO OBJETO

2.1. O presente tem como objeto a contratação em lote único de serviço para aquisição de solução de segurança da rede de dados do Conselho Regional de Medicina do Estado do Rio de Janeiro, composta por elementos de hardware e software, incluindo licenciamento, instalação, garantia e suporte técnico: em total conformidade com o **Edital n. 012/2017** e respectivo **Termo de Referência**, que ensejou este Contrato e Planilha de Preços da CONTRATADA datada de ___/__/18, partes integrantes deste instrumento independente de anexação.

CLÁUSULA TERCEIRA – OBRIGAÇÕES DO CONTRATANTE

3.1. Relacionar-se com a CONTRATADA, exclusivamente, por meio de pessoa por ela credenciada;

3.2. Prestar as informações e os esclarecimentos necessários ao bom andamento deste Contrato;

3.3. Efetuar os pagamentos à CONTRATADA na forma e nos prazos previstos neste Contrato, após o cumprimento das formalidades legais.

3.4. Nomear Fiscal responsável pelo acompanhamento e execução dos serviços, que deverá fazer anotações e registros de todas as ocorrências, determinando o que for necessário à regularização das falhas ou defeitos observados.

3.5. Ao CONTRATANTE caberá disponibilizar todos os meios e informações necessários para a entrega adequada do objeto deste Contrato, bem como efetuar o pagamento à CONTRATADA.

3.6. O CONTRATANTE exime-se de qualquer responsabilidade por danos causados pela CONTRATADA na entrega e/ou execução do objeto do presente contrato, respondendo a CONTRATADA por quaisquer danos eventualmente causados;

3.7. Fiscalizar a prestação dos serviços ora contratados, sem que daí advenha qualquer redução das obrigações e responsabilidades da CONTRATADA e, ainda, aplicar multa ou rescindir o contrato, caso a CONTRATADA desobedeça as presentes cláusulas.

3.8. De acordo com os artigos 73 e 76 da Lei nº 8.666/93, o objeto deste Contrato será recebido da forma como se segue:

a) Provisoriamente, imediatamente depois de efetuada a entrega, para efeito de posterior verificação de conformidade do produto com as especificações do Edital da Licitação;

b) Definitivamente, após verificação da sua conformidade com as especificações contidas na proposta apresentada e/ou no edital e seus anexos, no prazo máximo de 07 (sete) dias a contar do recebimento provisório.

3.9. A entrega do objeto pela empresa e seu recebimento pelo CREMERJ não implicam sua aceitação definitiva, que será caracterizada pela atestação da nota fiscal/fatura correspondente.

3.10. O recebimento definitivo ficará condicionado à observância de todas as cláusulas e condições fixadas neste instrumento e na proposta comercial, bem como ao atendimento de eventuais solicitações no sentido de que a CONTRATADA promova a substituição do objeto

entregue fora das especificações ou no qual venham a ser detectados defeitos, irregularidades ou imperfeições.

3.11. Constitui igualmente condição para a formalização do recebimento definitivo, a apresentação pela CONTRATADA de documento escrito onde constem às recomendações de uso, manutenção, conservação dos objetos entregues, bem como as relacionadas com as especificações técnicas destes.

3.12. Os objetos deste contrato serão recusados:

a) Quando entregues com especificações técnicas diferentes das constantes nos Anexos deste Contrato e na proposta comercial da CONTRATADA;

b) Quando apresentar qualquer defeito durante os testes de conformidade e verificação.

3.13. Ocorrendo a recusa, a CONTRATADA deverá providenciar a substituição do mesmo no prazo de entrega, contados da comunicação feita pelo CONTRATANTE.

3.14. O recebimento provisório ou definitivo não exclui a responsabilidade civil da CONTRATADA em face da lei e desta contratação.

3.15. Nos termos do art. 76 da Lei nº 8.666/93, o CONTRATANTE rejeitará, no todo ou em parte, o objeto deste Contrato executado em desacordo com as cláusulas contratuais e proposta comercial.

CLÁUSULA QUARTA – OBRIGAÇÕES DA CONTRATADA

4.1. OBRIGAÇÕES GERAIS

4.1.1. Assegurar a entrega dos objetos deste contrato em perfeitas condições, atendendo a legislação vigente, de acordo com o estabelecido no presente instrumento e Termo de Referência, no prazo de até 15 (quinze) dias corridos após a assinatura deste contrato, na sede do CREMERJ, localizada na Praia de Botafogo, nº 228, loja 119B, Botafogo, Rio de Janeiro/RJ;

4.1.2. Responsabilizar-se por todas e quaisquer despesas decorrentes de salários, encargos sociais, horas-extras, impostos, bem como quaisquer acidentes de que possam ser vítimas os seus empregados quando em serviço, e por tudo quanto a legislação vigente lhes assegure, inclusive férias, aviso prévio, indenização e quaisquer outros direitos;

4.1.3. Comprovar, sempre que solicitado pelo CONTRATANTE, o pagamento dos tributos, e/ou contribuições a ele atribuídos pela legislação tributária, trabalhista, previdenciária e parafiscal, inexistindo qualquer responsabilidade do CONTRATANTE.

4.1.4. Indicar o Responsável pela execução e acompanhamento do Contrato, a ser aceito pelo CONTRATANTE, conferindo-lhe poderes para representá-lo na execução do contrato. O Responsável será denominado de Preposto.

4.1.4.1. É função do Preposto:

a) coordenar, comandar e fiscalizar o bom andamento dos serviços;

b) cuidar da disciplina,

c) promover de forma harmoniosa a ligação e integração entre a CONTRATADA e a gerência designada pelo CONTRATANTE;

d) comunicar, por escrito, ao CONTRATANTE qualquer anormalidade de caráter urgente e prestar os esclarecimentos julgados necessários.

4.1.5. Prestar todos os esclarecimentos solicitados pelo CONTRATANTE, atendendo a todas as reclamações;

4.1.6. Responder pelas despesas resultantes de quaisquer ações, demandas, decorrentes de danos, seja por culpa sua ou qualquer de seus empregados e prepostos, obrigando-se, igualmente, por quaisquer responsabilidades decorrentes de ações judiciais de terceiros, que lhe venham a ser exigidas por força de lei, ligadas ao cumprimento do presente Contrato;

4.1.7. Não se obrigar perante terceiros, dando o presente contrato como garantia ou compensar direitos de créditos decorrentes da execução dos serviços ora pactuados em operações bancárias e/ou financeiras, sem prévia autorização expressa do CONTRATANTE;

4.2. OBRIGAÇÕES ESPECÍFICAS

4.2.1. Cumprir fielmente toda a execução do objeto, de acordo com as condições e exigências previamente estabelecidas;

4.2.2. Fornecer garantia dos equipamentos durante toda vigência Contratual;

4.2.3. Fornecer garantia dos hardwares/peças substituídos pelo prazo de 36 (trinta e seis) meses, sem prejuízo da garantia contratual;

4.2.4. Comunicar à CONTRATANTE qualquer anormalidade que esteja impedindo a execução contratual dos serviços de suporte, prestando os esclarecimentos julgados necessários;

4.2.5. Responsabilizar-se por todos os tributos, contribuições fiscais e parafiscais que incidam ou venham a incidir, direta ou indiretamente, sobre os serviços fornecidos, bem como pelo custo do frete e outros inerentes À execução do objeto, apresentando os documentos fiscais em conformidade com a legislação vigente;

4.2.6. Assumir todas as despesas com transporte, hospedagem e outros custos operacionais decorrentes da execução do objeto;

4.2.7. Responsabilizar-se pela fiel execução contratual, respondendo civil e criminalmente pelos danos diretos, que, por dolo ou culpa sua ou de seus empregados, causarem a CONTRATANTE ou a terceiros, sendo admitido o direito a ampla defesa;

4.2.8. Prestar serviços de suporte e assistência técnica aos bens pelo período de vigência do contrato, de acordo com a forma e regime estabelecidos;

4.2.9. Observar rigorosamente todos os prazos de atendimento e resolução de chamados estabelecidos, bem como as datas das visitas preventivas, sob pena de aplicação de multa e demais cominações pelo CREMERJ;

4.2.10. Agir de forma proativa, objetivando prevenir a ocorrência de erros e defeitos, por meio das inspeções nos equipamentos, componentes, dispositivos e softwares de configuração, bem como a coleta e avaliação de logs, atualização, verificação e inspeção visual das condições de funcionamento dos equipamentos, seus componentes e dispositivos;

4.2.11. Reparar eventuais falhas apresentadas nos equipamentos, compreendendo serviços de conserto, reparos e/ou substituição de bens, componentes e dispositivos, bem como sua configuração e gerenciamento, com vistas a normalidade da operação dos serviços prestados, em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados pela CONTRATADA;

4.2.12. Utilizar os manuais dos produtos e as diretrizes da TI da CONTRATANTE, para desinstalação, reconfiguração ou reinstalação de hardware e/ou software, atualização de versões de drivers, firmwares e software básico, correção de defeitos técnicos, ajustes e reparos necessários;

4.2.13. Prover toda e qualquer evolução de software, incluindo correções, patches, fixes, updates, service packs, novas releases, versions, builds e upgrades às suas expensas;

4.2.14. Utilizar nos serviços profissionais certificados pelo fabricante dos equipamentos, qualificados e tecnicamente capacitados nos produtos em questão;

4.2.15. Fornecer a sua equipe técnica todas as documentações, manuais, ferramentas e meios técnicos necessários para a execução do objeto, sem custos adicionais ao CREMERJ;

4.2.16. Fornecer novas versões e atualizações de firmware dos produtos, se houver, sem custos adicionais ao CREMERJ;

4.2.17. Trocar peças ou substituir peças/bens sempre que identificado ocorrências técnicas que justifiquem;

4.2.18. Fornecer peças novas e de primeiro uso, lacradas em sua embalagem original;

4.2.19. Abster-se de desativar hardware, software ou quaisquer outros recursos computacionais do CREMERJ, sem prévio conhecimento e autorização expressa da Administração;

4.2.20. Fornecer equipamento de redundância, com características iguais ou superiores, sempre que precisar desativar hardware, software ou quaisquer recursos computacionais do CREMERJ, até que o problema seja sanado;

4.2.21. Responder e ressarcir ao CREMERJ ou a terceiros por eventuais danos diretos causados, inclusive por seus empregados ou prepostos, na execução dos serviços;

4.2.22 Responsabilizar-se pelo sigilo e confidencialidade, por si e seus empregados, dos documentos e/ou informações que lhe chegarem ao conhecimento por força da execução do contrato, e tenham sido definidas como confidenciais, não podendo divulgá-lo, sob qualquer pretexto, conforme as diretrizes estabelecidas pela Política de Segurança da Informação e Comunicações do CREMERJ ou por qualquer normatização análoga ou que venha a substituir essa;

4.2.23. Disponibilizar uma infraestrutura de atendimento via telefone ou web, para recebimento e registro dos chamados técnicos realizados pelo CREMERJ, disponibilizando sempre um número de protocolo para controle de atendimento;

4.2.24. Entregar ao CREMERJ, às suas expensas, toda documentação técnica (relatórios técnicos) gerada em função da execução do Contrato;

4.2.25. Velar para que todos os privilégios de acesso a sistemas, dados ou informações do CREMERJ sejam utilizados exclusivamente na execução contratual, e pelo período estritamente essencial à realização de serviços;

4.2.26. Refazer ou corrigir serviços às suas expensas, no todo ou em parte, sempre que identificado pelo CREMERJ ter sido realizado em desacordo com o estabelecido no Termo de Referência;

4.2.27. Cumprir o cronograma de visitas programadas (manutenção preventiva) definido pelo CREMERJ;

4.2.28. Responder pelos danos causados diretamente ao CREMERJ ou a terceiros, decorrentes de sua culpa ou dolo, durante a execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização ou o acompanhamento pelo CREMERJ;

4.2.29. Responder por quaisquer danos causados diretamente aos equipamentos, softwares, informações e a outros bens de propriedade do CREMERJ, quando esses tenham sido ocasionados por seus técnicos durante a prestação dos serviços objeto desta contratação.

4.2.30. Durante o processo de implementação da solução de firewall, update de firmware da solução ofertada ou access points existentes testes de conformidade deverão ser executados individualmente visando a aferição da real capacidade técnica bem como a configuração de segurança atendendo as melhores praticas de segurança da informação buscando comprovar juntamente com a documentação do fabricante que os equipamentos de fato atendem aos requisitos constantes da especificação técnica. Nesse sentido, os testes serão efetuados em todos os itens de hardware e software da solução.

4.3. DA ESPECIFICAÇÃO DO SERVIÇO

4.3.1. ITEM 1: WatchGuard Firebox M570 Series Hardware - PN WGFBM570HW

4.3.1.1. SOBRE A SOLUÇÃO

4.3.1.1.1. Solução de segurança (appliance) Firewall – A **CONTRATADA** deverá implantar, fornecer, documentar, treinar e configurar uma solução de segurança baseada em solução de firewall do tipo appliance e demais ferramentas necessárias para promover a segurança da rede do **CONTRATANTE**, incluindo serviços de instalação, configuração de acordo com as necessidades do Conselho, suporte técnico e treinamento;

4.3.1.1.2. A **CONTRATANTE** pretende com esta contratação atender a necessidade de aquisição de um sistema de proteção de rede ininterruptamente ativo e de alta disponibilidade, com a adequação de suas funcionalidades, fazendo frente ao crescente número de acessos e novos tipos de ataques, através da implementação de um esquema de alta

disponibilidade do produto de Firewall para as conexões recebidas, estabelecimento e otimização de conexões VPN.

4.3.1.1.3. A solução de Firewall deverá possibilitar monitorar e controlar o tráfego de dados que circula entre a rede local e a Internet, estabelecendo um único canal de entrada e saída entre aqueles ambientes, permitindo a proteção da rede local (Intranet) contra ações de cracker e hackers.

4.3.1.1.4. A solução deverá prover proteção integrada de antivírus, Anti-Spyware, AntiSpam, Anti-Adware, Anti-Keylogger, filtro de conteúdo Web (Proxy) e controle inteligente de aplicações web;

4.3.1.1.5. Os equipamentos eletroeletrônicos devem aceitar tensão elétrica de entrada 110V, ou bivolt e atender a norma NBR 14136;

4.3.1.2. SOBRE OS EQUIPAMENTOS

4.3.1.2.1. Todos os equipamentos e respectivos acessórios e cabeamento especificados neste edital deverão ser novos, estarem em linha de produção do Fabricante e em perfeitas condições para sua instalação e operação imediata. Não serão aceitos produtos e equipamentos descontinuados pelos seus respectivos Fabricantes. Todos os equipamentos devem ser do mesmo Fabricante não sendo aceito nenhum tipo de garantia solidária.

4.3.1.2.2. Deverão ser entregues em embalagem individual lacrada, adequadamente protegida para transporte do mesmo com segurança.

4.3.1.2.3. Os equipamentos e respectivos acessórios deverão estar em conformidade com a presente especificação técnica do produto.

4.3.1.2.4. O equipamento a ser descrito tem a finalidade de atender o projeto de Tecnologia da Informação da **CONTRATANTE**, no quesito “Segurança e Gerência de Rede”, possibilitando o eficaz gerenciamento e controle dos links de Internet, gerenciamento, estabelecimento e otimização de conexões VPN, gerenciamento unificado de ameaças combinadas com prevenção de intrusão, antivírus, anti-spyware, AntiSpam e filtro de conteúdo web integradas.

4.3.1.2.5. Além dos equipamentos e especificações técnicas da Solução de Segurança descritas a seguir, é de responsabilidade da **CONTRATADA** ofertar e prever contemplação de outros equipamentos, cabos, módulos, conversores, softwares e licenças, hardware e/ou acessórios necessários para atender ao pleno funcionamento e com segurança apropriada para as

informações e toda a rede de computadores da **CONTRATANTE** devendo ser descriminado na proposta técnica/preço.

4.3.1.3. FUNCIONALIDADES GERAIS

4.3.1.3.1. Deve suportar três zonas de segurança (redes): externa, privada e opcional (DMZ mínimo de 5).

4.3.1.3.2. Deve suportar endereços IP estáticos e dinâmicos (DHCP e PPPoE) na interface externa.

4.3.1.3.3. O equipamento de firewall deve permitir DHCPv6 em interfaces externas.

4.3.1.3.4. O equipamento de firewall deve possuir um throughput de 8Gbps para firewall e 1.7Gbps para UTM (combinando GAV e IPS).

4.3.1.3.5. O equipamento de firewall deve suportar 9.200.000 conexões simultâneas.

4.3.1.3.6. O equipamento de firewall deve possuir funcionalidades de UTM, incorporando as funcionalidades de filtro de URL, IPS, GAV, Controle de Aplicação, DLP e proteção contra ameaças day-zero.

4.3.1.3.7. O equipamento de firewall deve possuir funcionalidades de um NgFW, incorporando as funcionalidades de filtro de URL, IPS, GAV, Controle de Aplicação, DLP e proteção contra ameaças day zero.

4.3.1.3.8. O equipamento de Firewall deve suportar a implementação de políticas de segurança de camada de aplicação.

4.3.1.3.9. Deve suportar em suas políticas de segurança em camada de aplicação (proxies) pré-configurados suportar os seguintes protocolos comuns: HTTP, HTTPS, POP3, SMTP, FTP, DNS, SIP, H323, TCP-UDP, TFTP.

4.3.1.3.10. O equipamento de firewall deve suportar autenticação via RADIUS, Secure ID, LDAP e Active Directory.

4.3.1.3.11. O equipamento de firewall deve suportar autenticação transparente de usuários de AD (Single SignOn).

4.3.1.3.12. O equipamento de firewall deve permitir habilitar e desabilitar SSLv3 em proxies de HTTPS/SMTP.

4.3.1.3.13. O equipamento de firewall deve suportar a configuração de regras de proxy explícito para aceitar solicitações de clientes e buscar informação em nome dos clientes.

4.3.1.3.14. O equipamento de firewall deve suportar a habilidade de web FTP por proxy explicito para utilizar comandos FTP nativos e enviar dados no formato HTTP response.

4.3.1.3.15. O equipamento de firewall deve suportar a habilidade de configurar um proxy SMTP para analisar documentos com macros embutidas e o equipamento também deve possuir uma opção para remover estes macros antes de enviar o documento para seus destinatários.

4.3.1.3.16. O equipamento de firewall deve possuir certificados digitais do tipo self-signed para executar deepinspection de pacotes via proxy SMTP sobre TLS.

4.3.1.3.17. O equipamento de firewall deve executar deepcontente inspection de dados em proxy HTTPS.

4.3.1.3.18. O equipamento de firewall deve limitar o acesso de usuários a site não permitidos pela política de segurança do CREMERJ.

4.3.1.3.19. O equipamento de firewall deve definir o intervalo de tempo entre tentativas de login incorretas por conexão FTP em clientes FTP e Server Proxy Actions.

4.3.1.3.20. O equipamento de firewall deve possuir a funcionalidade de NTP server e possuir uma política criada automaticamente de NTP para equipamentos conectados em sua rede interna.

4.3.1.3.21. O equipamento de firewall deve suportar DNS dinâmico.

4.3.1.3.22. O equipamento de firewall deve possuir defesas contra ataques fragmentados, permitindo que o firewall monte os pacotes fragmentados antes de encaminhá-los a redes internas.

4.3.1.3.23. O equipamento de firewall deve conseguir filtrar conteúdo nos protocolos mais comuns, assim como filtrar conteúdo tipo “MIME”.

4.3.1.3.24. O equipamento de firewall deve proteger e-mails internos contra open relay. Ele deve ser capaz e ser configurado para domínios de e-mail aceitos no ambiente.

4.3.1.3.25. O equipamento de firewall deve permitir a configuração de limites para detecção de ataques de flood e Denial of Service (DoS) além de distributed denial of service (DDoS).

4.3.1.3.26. O equipamento de firewall deve suportar Protocol Anomaly Detection (PAD) para DNS e outros tipos de protocolos.

4.3.1.3.27. O equipamento de firewall deve suportar Server Name Indication (SNI) para configurar domínios para funcionalidades de bloqueio, inspeção ou permissão.

4.3.1.3.28. O equipamento de firewall deve complementar capacidades e bloqueio de CN existentes com a finalidade de bloquear domínios específicos do Google.

4.3.1.3.29. O equipamento de firewall deve suportar bloqueio e gerenciamento de trafego por domínios especificados por FQDNs (FullyQualified Domain Names) a fim de bloquear sites disponibilizados por Content Delivery Networks (CDNs).

4.3.1.3.30. O equipamento de firewall deve suportar o bloqueio de domínios com configurações “wildcard”.

4.3.1.4. REQUISITOS VPN

4.3.1.4.1. A solução de UTM deve suportar VPN Mobile.

4.3.1.4.2. A solução de UTM deve suportar pelo menos 500VPNs Mobile usando IPSec.

4.3.1.4.3. A solução de UTM deve suportar ao menos 500 usuários mobile usando VPN SSL.

4.3.1.4.4. A solução de UTM deve permitir o download do cliente de VPN SSL através do próprio firewall.

4.3.1.4.5. A solução de UTM deve prover clientes SSL para Windows Vista, 7, 8, 10, MAC OS, Android e IOS.

4.3.1.4.6. A solução de UTM deve suportar VPN entre localidades (site-to-site VPN).

4.3.1.4.7. A solução de UTM deve suportar pelo menos 500VPNs entre escritórios utilizando IPSec.

4.3.1.4.8. A solução de UTM deve suportar iterações com outros produtos e marcas que suportam o padrão IPSec.

4.3.1.4.9. A solução de UTM deve suportar os seguintes métodos de autenticação: DES, 3DES, AES-128, AES-192, AES-256.

4.3.1.4.10. A solução UTM deve suportar os seguintes métodos de criptografia: SHA-2, MD5, IKE Pre-Shared Key, 3rd PartyCert.

4.3.1.4.11. A solução de UTM deve suportar DeadPeerDetection (DPD).

4.3.1.4.12. A solução de UTM deve suportar IKEv2.

4.3.1.4.13. A solução de UTM deve suportar Perfect Forward Secrecy (PFS) com chaves Diffie-Hellman (ou Diffie-Hellman-Merkle) em pacotes web e email.

4.3.1.4.14. A solução de UTM deve suportar VPN Failover (reestabelecer a VPN através de um segundo link em caso de falha do link primário).

4.3.1.4.15. A solução de UTM deve suportar VPN IPSEC com um throughput igual ou maior que 5.3 Gbps.

4.3.1.4.16. A solução de UTM deve permitir criar interfaces virtuais para VPNs e rotear trafego utilizando VPNs site-to-site com protocolos de roteamento dinâmico.

4.3.1.4.17. A solução de UTM deve suportar Branch Office VPN (BOVPN) de forma que uma interface virtual suporte qualquer interface como gateway local.

4.3.1.4.18. A solução de UTM deve suportar configuração de relatórios BOVPN que facilitem o troubleshooting.

4.3.1.4.19. A solução de UTM deve permitir visualizar estatísticas de VPN em interfaces virtuais, gateways, tunnel types, etc. para usuários mobile ou não.

4.3.1.4.20. A solução de UTM deve permitir visualizar mensagens de diagnóstico de VPN para ajudar a remediar e realizar o troubleshooting pelos administradores do sistema.

4.3.1.4.21. A solução de UTM deve suportar single-signon (SSO) em conexões de rede via tuneis BOVPN.

4.3.1.4.22. A solução de UTM deve suportar tuneis VPN site-to-site estáticos (políticas) e dinâmicas (roteadas) para soluções em nuvem.

4.3.1.5. FILTRAGEM DE CONTEÚDO

4.3.1.5.1. A solução de UTM deve suportar filtro de conteúdo via subscrição adicional.

4.3.1.5.2. A solução deve permitir que o filtro trabalhe por categorias, ajustado por grupos de usuário e possuir um mínimo de 120 categorias.

4.3.1.5.3. A solução de UTM deve permitir exceções no filtro de conteúdo por meio de whitelist.

4.3.1.5.4. A solução de UTM deve suportar uma base de dados localizada na nuvem e atualizada dinamicamente.

4.3.1.5.5. A solução de UTM deve filtrar conteúdo em múltiplas línguas, incluindo, mas não limitado a: português, inglês, alemão, espanhol, francês, italiano, holandês, japonês, chinês tradicional e simplificado.

4.3.1.5.6. A solução de UTM deve limitar o acesso de usuários a sites não permitidos pela política de segurança do CREMERJ.

4.3.1.6. LISTA DE BLACKLIST IPS

4.3.1.6.1. A solução de UTM deve suportar bloqueio de trafego vindo de IPs maliciosos reconhecidos por base de dados de blackslists disponíveis no mercado.

4.3.1.6.2. A solução de UTM deve suportar o bloqueio de trafego de botnets reconhecidos por base de dados de blacklist disponíveis no mercado.

4.3.1.7. CONTROLE DE APLICAÇÃO

4.3.1.7.1. A solução de UTM deve suportar a filtro de aplicação no próprio hardware UTM através de subscrição adicional.

4.3.1.7.2. A solução de UTM deve suportar a configuração de exceções para filtro de aplicação.

4.3.1.7.3. A solução de UTM deve ter suas assinaturas de aplicação atualizadas automaticamente e regularmente.

4.3.1.7.4. A solução de UTM deve identificar e bloquear mais de 1800 aplicações diferentes, incluindo controle granular de aplicação, como telas de login e metodologias específicas de transferência de arquivo.

4.3.1.7.5. A solução de UTM deve suportar updates automáticos de assinaturas de aplicação.

4.3.1.7.6. A solução de UTM deve updates de assinatura de aplicação em modo off-line.

4.3.1.8. REQUISITOS ANTIVÍRUS

4.3.1.8.1. A solução de UTM deve suportar a funcionalidade de antivírus de borda fornecida por fabricantes líderes no segmento de antivírus no mesmo equipamento UTM através de subscrição adicional.

4.3.1.8.2. A solução de UTM deve receber atualizações de assinaturas de antivírus automaticamente.

4.3.1.8.3. A solução de UTM deve suportar a opção de quarentena para e-mails recebidos.

4.3.1.8.4. A solução de UTM deve suportar whitelists para e-mails a fim de receber mensagens de domínios confiáveis em seu ambiente.

4.3.1.8.5. A solução de UTM deve ter a capacidade de detectar e bloquear spyware.

4.3.1.8.6. A solução de UTM deve ter a capacidade de detectar e bloquear vírus do tipo ransom.

4.3.1.8.7. A solução de UTM deve escanear todos os arquivos transferidos mesmo que os mesmos estejam dentro de diversos níveis de compressão (.zip, .tar, .rar, .gzip ou outras extensões de arquivos oriundos de outros compactadores).

4.3.1.8.8. A solução de UTM deve suportar os seguintes protocolos: HTTP, FTP, SMTP, POP3.

4.3.1.8.9. A solução de UTM deve suportar notas de reputação (1 a 100) para permitir o by-pass de escaneamento de URLs a fim de aumentar a performance da solução.

4.3.1.8.10. A solução de UTM deve bloquear automaticamente websites de reputação baixa (histórico de vírus, spam e outros tipos de malware) baseado em informações recebidas por um serviço disponível em nuvem.

4.3.1.8.11. A solução de UTM deve suportar um throughput de AntiVirus Gateway de pelo menos 3.2Gbps.

4.3.1.8.12. A solução de UTM deve suportar acesso a atualizações de assinaturas automaticamente, manualmente e de forma off-line.

4.3.1.9. REQUISITOS ANTISPAM

4.3.1.9.1. A solução de UTM deve possuir a funcionalidade de anti-spam através de subscrição adicional dentro do mesmo hardware UTM.

4.3.1.9.2. A solução de UTM deve permitir que seu anti-spam deve ser baseada na tecnologia RPD (Recurrent Pattern Detection).

4.3.1.9.3. A solução de UTM deve permitir que seu anti-spam deve prover capacidade de quarentena.

4.3.1.9.4. A solução de UTM deve permitir que seu anti-spam seja integrado com analise de antivírus spam (detecção de vírus outbreaks).

4.3.1.9.5. A solução de UTM deve suportar múltiplas línguas em seu spam-blocker.

4.3.1.9.6. A solução de UTM deve bloquear spam baseado em imagens e não apenas texto.

4.3.1.10. REQUISITOS IPS – INTRUSION PREVENT SYSTEM

4.3.1.10.1. A solução de UTM deve suportar a funcionalidade de IPS no mesmo equipamento via subscrição adicional.

4.3.1.10.2. A solução de UTM deve suportar atualizações automáticas de assinaturas de IPS.

4.3.1.10.3. A solução de UTM deve permitir que a solução de IPS realize analise em L7 (camada OSI 7) e defina o nível de severidade do ataque, gerando alarmos remotos e notificações de acordo.

4.3.1.10.4. A solução de UTM deve suportar bloqueio automático de fontes conhecidas de ataque.

4.3.1.10.5. A solução de UTM deve suportar os protocolos mais utilizados como HTTP, FTP, SMTP e POP3.

4.3.1.10.6. A solução de UTM deve suportar um throughput de IPS de pelo menos 5.5 Gbps.

4.3.1.10.7. A solução de UTM deve permitir o update manual e offline de assinaturas de IPS.

4.3.1.11. DATA LOSS PREVENTION

4.3.1.11.1. A solução de UTM deve proteger o ambiente contra perda de dados confidenciais (DLP) através de subscrição adicional.

4.3.1.11.2. A solução de UTM deve estar em compliance com as iniciativas de PCI e HIPAA.

4.3.1.11.3. A solução de UTM deve suportar regras predeterminadas de DLP a fim de identificar dados de cartão de credito, endereços e dados referentes a saúde e números de identificação pessoal.

4.3.1.11.4. A solução de UTM deve prever regras predeterminadas para ao mínimo 20 países diferentes.

4.3.1.11.5. A solução de UTM deve atualizar assinaturas de DLP (Data LossPrevention) de forma automática, online e manual, offline.

4.3.1.12. ADVANCED MALWARE DETECTION / ZERO DAY PREVENTION

4.3.1.12.1. A solução de UTM deve suportar a funcionalidade de detecção de malwares avançados no mesmo equipamento através de uma subscrição adicional.

4.3.1.12.2. A solução de UTM deve possuir um sistema completo de emulação para detecção de malware durante a o runtime da solicitação e, uma sandbox disponível em nuvem.

4.3.1.12.3. A solução de APT do UTM deve suportar todos os arquivos executáveis em Windows como: zip, PDF, Microsoft Office object, e arquivos Android APK.

4.3.1.12.4. A solução de UTM deve prover relatórios detalhes com analise identificando o arquivo como malware.

4.3.1.13. NETWORK DISCOVERY

4.3.1.13.1. A solução de UTM deve permitir aos administradores do firewall a enviarem pacotes UDP para escanear endpoints na rede.

4.3.1.13.2. A solução de UTM deve escanear os equipamentos conectados ao firewall, informar suas portas, endereço IP, endereço MAC, hostname, serviços e versão de sistema operacional.

4.3.1.13.3. A solução de escaneamento de rede deve possibilitar a detecção de equipamentos aprovados e rogue na rede.

4.3.1.14. MOBILE SECURITY

4.3.1.14.1. A solução de UTM deve permitir a configuração de requisitos mínimos para equipamentos iOS e Android para que estes trafeguem na rede.

4.3.1.14.2. A solução de UTM deve permitir o monitoramento e exigir que as configurações destes equipamentos móveis estejam em compliance com relação a versões de OS aprovadas, verificar se o hardware está rooted ou jaibroken além de escanear malware e adware em aparelhos Android.

4.3.1.14.3. A solução de UTM deve fornecer um dashboard consolidado para verificação de compliance dos dispositivos móveis.

4.3.1.14.4. A solução de UTM deve utilizar a funcionalidade de DHCP fingerprinting para determinar o tipo de dispositivo conectado na rede.

4.3.1.14.5. A solução de UTM deve ter compatibilidade ao modelo de Acess Point WatchGuard AP200.

4.3.1.15. NETWORK CAPABILITIES

4.3.1.15.1. O equipamento deve fornecer no mínimo as seguintes interfaces: 6x 10/100/1000BaseT e duas portas SFP 10/100/1000; Estas interfaces deve ser configuráveis como qualquer uma das três zonas de segurança informados no item 3.1.1.1.

4.3.1.15.2. O firewall deve suportar transceivers opticos que devem estar inclusos para todas as portas de fibra optica do produto.

4.3.1.15.3. O firewall deve suportar configuração de multi-wan, permitindo um mínimo de 04 conexões externas para a internet.

4.3.1.15.4. As interfaces do firewall devem suportar operação em modo fail-over.

4.3.1.15.5. As interfaces externas do firewall devem ser capazes de operar em modo round-robin com pesos customizáveis.

4.3.1.15.6. As interfaces externas do firewall devem ser capazes de operar em modo overflow, permitindo o uso de links externos quando a capacidade do link principal for excedia.

4.3.1.15.7. O equipamento de firewall deve suportar um mínimo de 500 VLANs.

4.3.1.15.8. O equipamento de firewall deve prover controle de banda definido por política, protocolo e grupo de usuários.

4.3.1.15.9. O equipamento de firewall deve possuir controle de banda por interface.

4.3.1.15.10. O equipamento de firewall deve possuir controle de banda por endereço IP e VLAN.

4.3.1.15.11. O equipamento de firewall deve permitir a configuração de cotas por tempo e trafego por usuário, podendo notificar o mesmo em caso de atingimento da cota estabelecida.

4.3.1.15.12. O equipamento de firewall deve suportar configuração em modo router (routing), drop-in (mesmo IP em todas suas interfaces) e em modo transparent bridge.

4.3.1.15.13. O equipamento de firewall deve suportar NAT estático, NAT dinâmico e 1-1 NAT.

4.3.1.15.14. O equipamento de firewall deve suportar alta disponibilidade em modo ativo-passivo e ativo-ativo.

4.3.1.15.15. O equipamento de firewall deve suportar policy-basedrouting (PBR), permitindo que os administradores especifiquem parâmetros para definir por qual interface externa o trafego da rede será enviado.

4.3.1.15.16. O equipamento de firewall deve suportar NAT e PAT.

4.3.1.15.17. O equipamento de firewall deve suportar Server LoadBalancing para servidores internos.

4.3.1.15.18. O equipamento de firewall deve suportar NAT estático (Portforwarding).

4.3.1.15.19. O equipamento de firewall deve suportar NAT dinâmico.

4.3.1.15.20. O equipamento de firewall deve permitir a implementação de NAT 1-1.

4.3.1.15.21. O equipamento de firewall deve suportar NAT Traversal para IPSEC.

4.3.1.15.22. O equipamento de firewall deve suportar policy-based NAT.

4.3.1.16. GESTÃO DA SOLUÇÃO

4.3.1.16.1. A solução de UTM deve prover administração em tempo real do equipamento via gerenciamento por interface gráfica.

4.3.1.16.2. A solução de UTM deve suportar o monitoramento em tempo real de logs gerados pelo equipamento.

4.3.1.16.3. A solução de UTM deve suportar o envio de diversos tipos de alerta através de SNMP ou email.

4.3.1.16.4. A solução de UTM suporta o uso de NAT para conexões via SNMP application layer gateway.

4.3.1.16.5. A solução de UTM deve suportar gerência através de múltiplos computadores simultaneamente.

4.3.1.16.6. A solução de UTM deve suportar VPN entre equipamentos, configurável via drag-and-drop.

4.3.1.16.7. A solução de UTM deve permitir a criação de templates de configuração VPN hub-and-spoke.

4.3.1.16.8. A solução de UTM deve suportar funcionalidade de “rollback” para configurações previas.

4.3.1.16.9. A solução de UTM deve suportar o protocolo de gerenciamento DVCP.

4.3.1.16.10. A solução de UTM deve suportar a edição de políticas de segurança de modo offline ou em GUI.

4.3.1.16.11. A solução de UTM deve permitir a edição de políticas através de Windows GUI e interface CLI.

4.3.1.16.12. A solução de UTM deve suportar diferentes níveis de administradores com acessos distintos.

4.3.1.16.13. A solução de UTM deve suportar autenticação com Windows Active Directory.

4.3.1.16.14. A solução de UTM deve suportar a gerência via web browser.

4.3.1.16.15. A solução de UTM deve suportar login via SSO (single-signon) para RDP.

4.3.1.16.16. A solução de UTM deve suportar MS Exchange Server 2013 para SSO Exchange Monitor.

4.3.1.16.17. A solução de UTM deve suportar a troca de múltiplos usuários utilizando um cliente SSO instalado em Windows Vista, Windows 7, Windows 8, Server 2008, Server 2012, Server 2016.

4.3.1.16.18. A solução de UTM deve suportar equipamentos que são gerenciados via linha de comando, porta serial ou SSH.

4.3.1.16.19. A solução de UTM deve suportar interface de usuário via web para gerência do equipamento, devendo ser compatível com tablets e outros equipamentos móveis.

4.3.1.16.20. A solução de UTM deve suportar o rastreamento de configuração e deve permitir a indicação das diferenças entre duas configurações salvas em datas diferentes.

4.3.1.16.21. A solução de UTM deve suportar a criação de arquivos de configuração offline sem estar diretamente conectado ao firewall.

4.3.1.16.22. A solução de UTM deve suportar a instalação em ambientes remotos sem a necessidade de funcionário com conhecimento técnico on-site. O produto deve possuir capacidade de baixar uma configuração armazenada na nuvem quando o equipamento for iniciado pela primeira vez.

4.3.1.16.23. A solução de UTM deve permitir a mudança da interface externa por meio de um arquivo CSV.

4.3.1.16.24. A solução de UTM deve suportar SSO para Radius em um servidor fornecido separadamente.

4.3.1.16.25. A solução de UTM deve rastrear a sessões de usuário através da funcionalidade de SSO Radius.

4.3.1.16.26. A solução de UTM deve destacar as diferenças entre versões de configuração do firewall.

4.3.1.17. LOGS E RELATÓRIOS

4.3.1.17.1. A solução de UTM deve permitir a implementação de servidores externos de maneira que todos os logs e relatórios sejam armazenados de forma centralizada.

4.3.1.17.2. A solução de UTM não deve ter custos adicionais para armazenamento e criação de logs e relatórios.

4.3.1.17.3. A solução de UTM deve suportar TCP (Transport Control Protocol) e utilizar uma base de dados SQL para garantir escalabilidade.

4.3.1.17.4. A solução de UTM deve suportar o envio de LOGs simultaneamente e múltiplos servidores de log.

4.3.1.17.5. A solução de UTM deve permitir a configuração de servidores de LOG backup, que serão utilizados caso o servidor primário apresente falhas.

4.3.1.17.6. A solução de UTM deve criptografar a transmissão de logs dos firewall para seu envio ao servidor sem a necessidade de VPN.

4.3.1.17.7. A solução de UTM deve possuir mais de 90 relatórios predefinidos sem qualquer custo extra ou adicional.

4.3.1.17.8. A solução de UTM deve alertar o administrador da rede quando a base de dados de log e relatórios atingir um valor próximo ao seu limite estipulado.

4.3.1.17.9. A solução de UTM deve suportar a extração de relatórios nos formatos PDF e CSV.

4.3.1.17.10. A solução de UTM deve possuir relatórios de compliance para HIPAA e PCI.

4.3.1.17.11. A solução de UTM deve elaborar relatórios automaticamente assim como seu envio por e-mail.

4.3.1.17.12. A solução de UTM deve possuir um relatório executivo com informações de “High Level”.

4.3.1.17.13. A solução de UTM deve permitir a execução de pivot e drilldown em informações mais detalhadas a partir de qualquer item logado.

4.3.1.17.14. A solução de UTM deve suportar o envio automático de todos os tipos de relatórios por e-mail.

4.3.1.17.15. A solução de UTM deve suportar controle de acesso por usuário com a finalidade de garantir o devido acesso e ações tomadas por usuário.

4.3.1.17.16. A solução de UTM deve possuir imagens virtuais da solução de relatório e armazenamento de logs.

4.3.1.17.17. A solução de armazenamento de logs e relatórios deve ser compatível com VMware.

4.3.1.17.18. A solução de UTM deve possuir uma visão tipo “treemap” para indicar o tipo de trafego passando pelo equipamento de forma gráfica.

4.3.1.17.19. A solução de UTM deve suportar uma solução de visibilidade de demonstre em um mapa mundi a origem e destino de trafego de aplicações, trafego negado, e eventos de IPS.

4.3.1.17.20. A solução de UTM deve suportar relatórios de IPS que indiquem informações detalhadas e referencias CVE para cada evento alertado.

4.3.1.17.21. A solução de UTM deve permitir agregar diversos firewalls em forma de grupos.

4.3.1.17.22. A solução de UTM deve suportar o log de Single SignOn (SSO) para melhorar a monitoria.

4.3.1.17.23. A solução de UTM deve suportar o monitoramento de logs de loadbalancing e de eventos instalados em múltiplos domínios.

4.3.1.17.24. A solução de UTM deve suportar um agente SSO que envie uma resolução de DNS para resolver o nome do host para aquele endereço IP e determinar em qual domínio o cliente pertence.

4.3.1.17.25. A solução de visibilidade deve suportar visibilidade por FQDN em forma de relatório através do equipamento de firewall.

4.3.1.17.26. A solução de visibilidade deve demonstrar o volume de banda e tempo utilizado por usuário em forma de relatório acessível através do equipamento ou via web UI.

4.3.1.17.27. A solução de visibilidade deve possuir um dashboard com a habilidade de bloquear a origem de um ataque por IP diretamente pelo painel.

4.3.1.17.28. A solução de UTM deve permitir que o painel de visibilidade tenha funções para criação de políticas de firewall.

4.3.1.17.29. A solução de UTM deve possuir um relatório indicando o uso de cada política, inclusive as políticas não utilizadas no firewall.

4.3.1.17.30. A solução de UTM deve possuir um painel de visualização que efetivamente demonstre, de forma geográfica, o destino de trafego que passa pelo firewall e as políticas que foram acionadas.

4.3.2. Item 2: Trade Up to WatchGuard Firebox M570 with 3-yr - Total Security Suite (Software Only) - PN WGTM570MD3TU

A rede precisa de mecanismos de varredura para se proteger contra sypware, vírus, aplicativos maliciosos e vazamento de dados incluindo ramsomware, botnets, ameaças persistentes avançadas e malware. A solução de rede lidará com todos os aspectos de prevenção de ameaça, detecção, correlação e resposta o quanto antes à medida que essas ameaças evoluem, incluindo, sem limitação a prevenção e resposta imediata contra ransomware e malwares avançados. O Total Security Suite possui além da proteção de malware avançada, proteção contra perda de dados, recursos aprimorados de visibilidade de rede e a capacidade de agir contra ameaças diretamente na plataforma. Também deve incluir suporte de nível de *Gold* 24x7. Além disso, todos os serviços tradicionais de segurança de rede típicos de um *appliance* UTM devem estar presentes: IPS, GAV, filtragem de URL, controle de aplicativos, bloqueio de spam e pesquisa de reputação.

4.3.2.1. ESPECIFICAÇÃO DO TOTAL SECURITY SUITE

4.3.2.1.1. SERVIÇOS DE SEGURANÇA INCLUSOS NO TOTAL SECURITY SUITE

4.3.2.1.1.1. SERVIÇO DE PREVENÇÃO DE INTRUSÕES (IPS)

O IPS usa assinaturas atualizadas continuamente para varrer o tráfego na maioria dos protocolos para fornecer proteção em tempo real contra ameaças, incluindo spyware, injeções de SQL, script entre sites e estouro de buffer.

4.3.2.1.1.2. SERVIÇO REPUTATIONENABLED DEFENSE (RED)

Um serviço de busca de reputação baseado em nuvem que protege os usuários da web de sites e botnets maliciosos, aprimorando drasticamente o processamento de web.

4.3.2.1.1.3. FILTRAGEM DE URLWEBBLOCKER

Além de bloquear automaticamente sites maliciosos conhecidos, o conteúdo granular do WebBlocker e as ferramentas de filtragem de URL permitem que você bloqueie conteúdos inadequados, conserve a largura de banda da rede e aumente a produtividade dos funcionários.

4.3.2.1.1.4. SPAMBLOCKER

Detecção de spam em tempo real para proteção contra surtos. O spam Blocker é tão rápido e eficaz que consegue analisar até 4 bilhões de mensagens por dia.

4.3.2.1.1.5. ANTIVÍRUS DO GATEWAY(GAV)

Avalie nossas assinaturas atualizadas continuamente para identificar e bloquear spywares, vírus, cavalos de troia, rogueware e ameaças combinadas conhecidos, incluindo as novas variantes dos vírus conhecidos. Ao mesmo tempo, a análise heurística rastreia dados, construções e ações suspeitos para garantir que os vírus desconhecidos não passem despercebidos.

4.3.2.1.1.6. CONTROLE DE APLICATIVOS

Permita, bloqueie ou restrinja o acesso a aplicativos de forma seletiva com base no departamento do usuário, função e horário do dia e veja, em tempo real, o que está sendo acessado na sua rede e por quem.

4.3.2.1.1.7. PREVENÇÃO DE PERDADE DADOS (DLP)

Este serviço impede perda de dados maliciosa ou acidental verificando textos e tipos de arquivo comuns para detectar informações confidenciais que tentam sair da rede.

4.3.2.1.1.8. APT BLOCKER – PROTEÇÃO AVANÇADA CONTRA MALWARE

O APT Blocker usa uma simulação de última geração para detectar e impedir a maioria dos ataques sofisticados, incluindo ransomware, ameaça de primeiro dia e outros malwares avançados.

4.3.2.1.1.9. DIMENSION COMMAND

O Dimension traduz os dados coletados de todos os dispositivos na rede em inteligência acionável sobre a rede e as ameaças. O Dimension Command fornece a capacidade de tomar uma medida para aliviar essas ameaças instantaneamente de um console central.

4.3.2.1.1.10. DESCOBERTA DE REDE

Um serviço baseado em assinatura para os dispositivos Firebox que gera um mapa visual de todos os nós na sua rede para que seja possível ver com facilidade onde há riscos presentes.

4.3.2.1.1.11. THREAT DETECTION AND RESPONSE

Correlacione eventos de segurança de terminal e rede com inteligência contra ameaças de grau empresarial para detectar, priorizar e ativar a ação imediata para impedir ataques de malware, evoluindo o modelo existente para estender a prevenção passada incluindo correlação, detecção e resposta.

4.3.2.1.1.12. SUPORTE

O suporte deve ser prestado dentro das 24 (vinte e quatro) horas do dia pelos 7 (sete) dias da semana.

4.3.3. Item 3: WatchGuard Firebox AP320 Hardware – PN WGAP320HW

4.3.3.1. ESPECIFICAÇÃO TÉCNICA DO *ACCESS POINT* - PONTOS DE ACESSO DE REDE SEM FIO

4.3.3.1.1. Possibilitar operar com modelos de 1 ou 2 rádios;

4.3.3.1.2. Suportar frequências de 2.400-2.474GHz, 5.150-5.250GHz, 5.250-5.350GHz, 5.470-5.725GHz, 5.725-5.850GHz;

4.3.3.1.3. Possuir 6 antenas omnidirecionais;

4.3.3.1.4. Trabalhar com velocidade de dados de 1.3 Gbps para padrão 11ac e de 450 Mbps para padrão 11n;

4.3.3.1.5. Deve suportar temperaturas entre 0 e 40 graus centigrados;

4.3.3.1.6. Possuir energização em PoE 802.3af/at ou Adaptador A/C;

4.3.3.1.7. Suportar no mínimo 16 SSID no mesmo equipamento;

4.3.3.1.8. Suportar os seguintes padrões IEEE: 802.11a/b/g/n/ac, 802.11i, 802.1q, 802.1X, 802.3af/at, 802.11e;

4.3.3.1.9. O gerenciamento da rede sem fio não deve adicionar nenhum equipamento adicional (função controller) na solução oferecida, devendo ser tratado pelo appliance UTM físico ou virtual;

4.3.4. Item 4: WatchGuard AP320 and 3-yr Standard Support - PN WGLAP320MD3

4.3.4.1. Os Access points devem ter garantia, atualização e suporte de 36 (trinta e seis) meses.

4.3.5. Item 5: WatchGuard AP200 1-yr LiveSecurity Renewal PN WG019818

4.3.5.1. SERVIÇOS ASSEGURADOS NA EXTENSÃO DA GARANTIA

4.3.5.1.1. A extensão de garantia atenderá aos seguintes itens:

4.3.5.1.1.1. Deve contemplar a substituição do equipamento em caso de problema físico.

4.3.5.1.1.2. Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:

a. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento;

b. Deve assegurar a utilização de novas/atualizações de versões de software da solução sem ônus a Licitante;

c. Deve permitir o acesso à base de conhecimento da solução;

4.3.6. Item 6: Instalação

ETAPAS DA INSTALAÇÃO:

Item	Descrição
1	Instalação física dos modelos adquiridos: M570, AP320 e remanejamento do AP200 para outros locais
	Configuração do M570
	Configuração e atualização dos APs já existentes na nova solução (Modelo já instalado AP200) e dos AP320.
	Atualização de firmware da solução de segurança
	Configuração de ambiente de segurança aderente às políticas do cliente
	Configuração de servidor de relatórios
	Passagem de conhecimento para a equipe
	Documentação

4.3.6.1. SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO DE SEGURANÇA

4.3.6.1.1. Quanto aos serviços:

4.3.6.1.1.1. A **CONTRATADA** deverá preparar, instalar e configurar a solução ofertada, na Sede do CREMERJ.

4.3.6.1.1.2. A instalação da solução de segurança de rede deverá ser feita por profissionais devidamente qualificados e certificados na área de segurança do fabricante.

4.3.6.1.1.3. A prestação dos serviços de instalação e configuração deverá compreender entre outros, os seguintes procedimentos: Análise da topologia e arquitetura da rede da **CONTRATANTE**, considerando os ativos de rede instalados, acesso à Internet, sites remotos (subsedes e seccionais na capital e no interior, CFM (Conselho Federal de Medicina)), serviços de rede oferecidos aos usuários internos e externos, regras de firewall existentes, bem como qualquer outro equipamento ou sistema relevante na segurança do perímetro, sendo então feita a configuração da solução de segurança de acordo com as exigências levantadas, visando:

4.3.6.1.1.3.1. Facilitar o gerenciamento e a solução de eventuais problemas, com a proposição de eventuais correções na topologia da rede e implementação de alguns protocolos com a finalidade de minimizar os riscos e aumentar a disponibilidade do sistema.

4.3.6.1.1.3.2. Realizar o projeto de segurança do perímetro, considerando todos os serviços fornecidos aos usuários internos e externos da **CONTRATANTE**.

4.3.6.1.1.3.3. Emissão de relatório, contendo todas as informações coletadas e a sugestão de configuração.

4.3.6.1.1.3.4. Aplicação de todas as funcionalidades definidas no projeto e implantação do gerenciamento da solução.

4.3.6.1.1.3.5. Realização de testes de funcionamento.

4.3.6.1.1.4. Durante toda a implantação do projeto, o técnico da **CONTRATADA** deverá demonstrar à equipe técnica de acompanhamento da **CONTRATANTE** como instalar e configurar a solução e/ou softwares fornecidos (instalação assistida). Esta demonstração deverá contemplar os conceitos das tecnologias utilizadas pelo equipamento e a operação dos principais recursos dos produtos entregues.

4.3.6.1.1.5. Todo o processo de instalação e configuração do sistema deverá ser documentado pela **CONTRATADA** sob a forma de relatório ou roteiro, de forma que a equipe técnica da **CONTRATANTE** possa reproduzir a instalação da solução de segurança quando necessário consultando a documentação.

4.3.6.1.1.6. Deverão ser configuradas todas as características disponíveis nos produtos fornecidos e solicitadas pela **CONTRATANTE**.

4.3.6.1.1.7. Todas as configurações de regras, políticas, Black e White list, VPNs implantadas e configuradas no firewall atual deverão ser importadas ou reconfiguradas no novo firewall de forma que os serviços não sejam impactados.

4.3.6.1.1.8. Os Access points existentes devem ser atualizados para ultima versão do firmware e configurado no novo equipamento de firewall mantendo a política atual utilizando as melhores praticas de segurança dentro do novo ambiente.

4.3.6.1.1.9. A instalação e configuração definitivas do software para segurança de rede (entrada definitiva em produção substituindo o sistema existente) poderão ser feitas fora do horário normal de expediente da **CONTRATANTE**, (segunda à sexta de 09:00 às 18:00h), se necessário, a fim de minimizar o impacto da migração nos ambientes de trabalho. Tais atividades ocorrerão sem ônus adicional à **CONTRATANTE**.

4.3.6.1.1.10. Todos os equipamentos deverão passar por testes individualizados e integrados garantindo a correta implementação seguindo todos os *baselines* apresentados pela solução assegurando o nível aceitável de segurança da informação para a organização.

4.3.7. Qualificação técnica

4.3.7.1. Como qualificação técnica, a **CONTRATADA** deverá apresentar juntamente com os documentos de habilitação, a seguinte documentação:

4.3.7.1.1. Atestado de capacidade técnica emitida por instituição ou empresa de direito público ou privado no Brasil, impresso em papel timbrado (não serão aceitas declarações genéricas de catálogos, manuais ou Internet), com nome e telefone de contato dos responsáveis pela informação atestada, comprovando que a licitante forneceu solução de características semelhantes ao especificado neste termo de referência, prestando a devida garantia e suporte técnico. O documento deverá ainda atestar a satisfação da instituição ou empresa de direito público ou privado no Brasil com o produto ofertado pela licitante.

4.3.8. Garantia

4.3.8.1. A garantia deverá ser de **TRINTA E SEIS (36) meses**.

4.3.8.2. Deve contemplar a substituição do equipamento em caso de problema físico.

4.3.8.3. Deve contemplar suporte do Fabricante pelo período vigente. Com no mínimo, as seguintes características:

4.3.8.3.1. O suporte do fabricante deve ter um sistema de abertura de chamados para acompanhamento; Deve assegurar a utilização de novas versões de software da solução sem ônus a **CONTRATANTE.**

4.3.8.3.2. Deve permitir o acesso à base de conhecimento da solução;

4.3.8.3.3. A **CONTRATADA** deverá garantir junto ao fabricante a prestação de serviços de garantia no termo contratual da solução de segurança de rede, sem ônus adicionais à **CONTRATANTE**, compreendendo os defeitos decorrentes de projeto, fabricação, construção, montagem, acondicionamento, ou outro qualquer durante o período de operação.

4.3.8.3.4. Deverão estar abrangidos pela garantia ainda, os serviços de identificação dos componentes, peças e materiais responsáveis pelo mau funcionamento do sistema.

4.3.8.3.5. A garantia deverá ser pelo período de, no mínimo, 36 (trinta e seis) meses a contar da data do TERMO DE RECEBIMENTO DEFINITIVO.

4.3.8.3.6. Os serviços de garantia dos equipamentos deverão ser prestados por empresa credenciada pelo fabricante dos produtos fornecidos.

4.3.8.3.7. Durante o período de garantia (trinta e seis meses), a **CONTRATADA** deverá garantir junto ao fabricante sem ônus para a **CONTRATANTE**, o fornecimento das atualizações (*patches*) corretivas do software e firmware dos equipamentos fornecidos, bem como o recebimento de atualizações (assinatura) do software da solução de segurança.

4.3.8.3.8. A **CONTRATADA** deverá garantir junto ao fabricante a prestação dos serviços de garantia nas seguintes condições:

4.3.8.3.8.1. Os serviços serão solicitados à Central de Atendimento indicada pela **CONTRATADA**, por meio de abertura de chamado técnico efetuada por técnicos da **CONTRATANTE**.

4.3.8.3.8.2. Os componentes, peças e materiais que substituírem os defeituosos deverão ser originais do fabricante e de qualidade e características técnicas iguais ou superiores aos existentes no equipamento.

4.3.8.3.8.3. Caso o equipamento defeituoso não possa ser consertado no prazo descrito ou deva ser reparado em laboratório, o FABRICANTE deverá providenciar substituição temporária, do equipamento,

instalando e configurando outro equipamento idêntico, de forma que não haja interrupção nas atividades dos usuários.

4.3.8.3.8.4. A **CONTRATADA** deverá garantir junto ao o FABRICANTE que eventuais reparos em laboratório, o deslocamento de equipamentos e seu retorno ao local de origem serão de responsabilidade do FABRICANTE.

4.3.8.3.8.5. Os serviços prestados em garantia, incluindo as substituições de hardware, não terão qualquer ônus adicional para a **CONTRATANTE**.

4.3.9. Prazo para atendimento

4.3.9.1. Prazo para atendimento e solução de problemas referentes à garantia e suporte técnico

4.3.9.1.1. Em caso de problemas detectados nos sistemas ofertados considere-se o seguinte:

4.3.9.1.1.1. Caso haja suspensão total no funcionamento das soluções compostas por essas ferramentas, o atendimento e suporte que a **CONTRATADA** deverá garantir junto ao FABRICANTE deverão obedecer aos seguintes prazos:

a) para o atendimento ao chamado: 2 (duas) horas;

b) para a solução do problema: 6 (seis) horas;

4.3.9.1.1.2. Caso o problema detectado não tenha causado a suspensão total no funcionamento das soluções compostas por essas ferramentas, os prazos serão os que seguem:

a) para o atendimento ao chamado: 2 (duas) horas;

b) para a solução do problema: 24 (vinte e quatro) horas;

4.3.10. Serviços de suporte técnico da solução de segurança após implementação

4.3.10.1. A **CONTRATADA** deverá prestar serviços de suporte técnico pelo período mínimo de 90 dias contados a partir da data do TERMO DE RECEBIMENTO DEFINITIVO sem quaisquer ônus adicionais à **CONTRATANTE**, que abrangerá:

i. Auxiliar na análise, utilização e configuração da solução.
ii. Auxiliar na identificação é solução de problemas em software e hardware.
iii. Auxiliar na instalação e configuração de atualizações de firmware e software (patches), bem como de novas versões dos produtos;
iv. Auxiliar na auditoria e análise de logs.
v. Encaminhar, a pedido da **CONTRATANTE** incidentes ao fabricante da solução.
vi. Os serviços serão solicitados à Central de Atendimento indicada pela **CONTRATADA**, por meio de abertura de chamado técnico efetuada por técnicos da **CONTRATANTE**.
vii. Os serviços poderão ser prestados na modalidade de atendimento remoto, por meio de chamados.
viii. Os técnicos da **CONTRATANTE** deverão ter acesso à base de conhecimento dos produtos ofertados, via website do fabricante, visando obter informações sobre a solução de segurança fornecida.
ix. Os serviços de suporte técnico não terão qualquer ônus adicional para a **CONTRATANTE**.

4.3.11. Condições de recebimento das licenças e dos equipamentos

4.3.11.1. As licenças e os equipamentos deverão ser entregues em no máximo 15 (quinze) dias, contados a partir do recebimento pela Adjudicatária da convocação expressa encaminhada pela **CONTRATANTE** juntamente com a Nota de Empenho.

4.3.12. Da entrega

4.3.12.1. A entrega deverá ser na Sede do Conselho Regional de Medicina do Estado do Rio de Janeiro, localizada na Praia de Botafogo, 228 / Lj 119B, Botafogo – Rio de Janeiro, RJ, CEP 22.250-145, no horário de 09h00 às 17h00.

CLÁUSULA QUINTA – DO VALOR

5.1. Pelos produtos e/ou serviços a serem entregues pela CONTRATADA, a CONTRATANTE pagará o preço unitário, constante da Planilha de Preços que ensejou o julgamento da proposta da CONTRATADA como vencedora no Pregão nº 001/2018, **multiplicado pelo número de quantidade solicitadas para entrega, conforme abaixo:**

ITEM	OBJETOS	QUANT.	VALOR MÁX. UNIT.
1	**WatchGuard Firebox M570 Series Hardware - PN WGFBM570HW**	**1 (um)**	**R$ XXX**
2	**Trade Up to WatchGuard Firebox M570 with 3-yr Total Security Suite (Software Only) - PN WGTM570MD3TU**	**1 (um)**	**R$ XXX**
3	**WatchGuard Firebox AP320 Hardware - PN WGAP320HW**	**5 (cinco)**	**R$ XXX**
4	**WatchGuard AP320 and 3-yr Standard Support - PN WGLAP320MD3**	**5 (cinco)**	**R$ XXX**
5	**WatchGuard AP200 1-yr LiveSecurity Renewal PN WG019818**	**7 (sete)**	**R$ XXX**
6	**- Instalação física e configuração - Atualização de Firmware da Solução de Segurança - Configuração de ambiente de segurança aderente as políticas do cliente - Configuração de Servidor de Relatórios - Passagem de conhecimento - Documentação**	**1 (um)**	**R$ XXX**

5.2. O preço unitário referido no item acima, inclui todos os serviços, materiais, encargos, frete tributos ou quaisquer outros de outras naturezas e a remuneração da CONTRATADA, relacionados aos serviços a serem prestados pela CONTRATADA.

5.3. Para todos os efeitos, inclusive imposição de penalidades, o valor total estimado deste contrato é de R$_____ (xxxxxxxxxx → *valor global da proposta*).

CLÁSULA SEXTA – DAS CONDIÇÕES DE FATURAMENTO E PAGAMENTO

6.1. A CONTRATADA faturará após a efetiva entrega dos produtos/serviços;

6.2. O pagamento será efetuado em até 20 (vinte) dias corridos, a contar do recebimento da Nota Fiscal devidamente discriminada em nome do Conselho Regional de Medicina do Estado do Rio de Janeiro, CNPJ n.º 31.027.527/0001-33, após a perfeita execução dos serviços contratados, constando o número do Processo (nº 039/2017) e o número do Pregão (nº 001/2018), acompanhada dos seguintes documentos, sem o qual, havendo atraso dos mesmos, ensejará a contagem de novo prazo para pagamento:

6.2.1. Declaração do Simples *(assinada e original)*, *caso a empresa seja Optante do SIMPLES Nacional*;

6.2.2. Certidão de Regularidade do FGTS, Certidão específica quanto à inexistência de débito de contribuições junto ao INSS, Certidão Conjunta de Débitos Relativos a Tributos Federais e à Dívida Ativa da União, conforme Decreto n.º 6.106/2007;

6.3. O pagamento poderá ser feito através de boleto bancário ou depósito, sendo neste último caso, necessário que conste na descrição da Nota Fiscal os dados: Banco, Agência e Conta para depósito, cuja titularidade deve estar em nome da empresa vencedora deste certame licitatório.

6.4. A liberação da Nota Fiscal/Fatura para pagamento ficará condicionada ao atesto do(s) Fiscal(is), conforme disposto nos artigos 67 e 73 da Lei n. º 8.666/93;

6.5. Qualquer atraso ocorrido na apresentação dos documentos exigidos nos Itens **6*.2.1, 6.2.2*** e ***6.3,*** deste contrato, **importará em prorrogação automática do prazo de vencimento** da obrigação do CREMERJ até sanada todas as pendências.

6.6. Fica a CONTRATADA ciente de que, quando da ocasião do pagamento, serão verificados se as condições de habilitação estão mantidas, sem as quais ocorrerá prorrogação automática do prazo de vencimento da obrigação do CREMERJ até que a regularidade seja comprovada.

6.7. Fica a empresa CONTRATADA ciente da obrigatoriedade de apresentação do Termo de Opção pelo Simples, quando assim couber, no ato da entrega da Nota Fiscal, esclarecendo o CREMERJ que a não apresentação do documento em questão, ocasionará o desconto no pagamento devido à empresa do valor referente ao encargo previsto na Lei nº 9.430 de 27/12/96.

6.8. Todos os impostos serão retidos em conformidade com a IN-RFB nº 1.234, de 11 de janeiro de 2012 e suas alterações posteriores.

6.9. O preço ofertado na licitação será fixo e irreajustável durante sua vigência, cabendo a empresa VENCEDORA, mantê-lo para a execução na íntegra do objeto contratual, para a realização dos dois eventos no preço constante da proposta apresentada.

CLÁUSULA SÉTIMA – DA FISCALIZAÇÃO DO CONTRATO

7.1. A fiscalização e o acompanhamento do contrato e execução dos serviços serão realizados pelo(s) Sr(s). XXXXX, Fiscal(is) deste contrato, especialmente designado(s) pelo CREMERJ na forma do Artigo 67 da Lei nº 8.666/93.

CLÁUSULA OITAVA – RECURSOS FINANCEIROS

8.1. As despesas com a execução do presente Contrato correrão à conta das dotações orçamentárias destinadas ao CONTRATANTE para o corrente exercício de 2018, assim classificados:

- Natureza das Despesas : Financeira
- Fonte de Recurso: Orçamento
- Nota de Empenho nº: xxx/2018
- Rubrica Orçamentária nº: xxxxxxxxxxxx
- Valor Total do Contrato: R$ XXXXXX *(xxxxxxxx)*

CLÁUSULA NONA – VIGÊNCIA

9.1. O presente contrato vigorará pelo prazo de 12 (doze) meses, a partir da data de sua assinatura, podendo ser alterado através de Termo Aditivo, respeitado os limites da Lei nº 8.666/93.

9.2. A garantia do objeto deste contrato deverá ser de **36 (trinta e seis) meses** a contar da data do TERMO DE RECEBIMENTO DEFINITIVO.

CLÁUSULA DÉCIMA– DOCUMENTOS INTEGRANTES

10.1. Fazem parte integrante do presente contrato, a Proposta de Preços da CONTRATADA, o Edital do Pregão N. 001/2018 e seus anexos e demais elementos que o acompanham, independentemente de anexação.

CLÁUSULA DÉCIMA PRIMEIRA – DA ALTERAÇÃO CONTRATUAL

11.1. As alterações ao presente Contrato serão feitas através de ADITAMENTO assinado pelo CONTRATANTE e pela CONTRATADA, com base no disposto no artigo 65 da Lei n. 8.666/93.

CLÁUSULA DÉCIMA SEGUNDA - DA INEXECUÇÃO

12.1. A inexecução total ou parcial do presente Contrato ensejará a sua rescisão, com as consequências por este previstas e, especialmente, as consequências dos artigos 78 a 80 da Lei n. 8.666/93 e suas alterações.

CLÁUSULA DÉCIMA TERCEIRA - DA MULTA

13.1. Pela inexecução total ou parcial das cláusulas e condições previstas no presente Contrato, no Edital do Pregão Presencial e na Proposta da CONTRATADA, o CONTRATANTE poderá, garantida a defesa prévia, aplicar à CONTRATADA as sanções previstas nos artigos 86 e 87 da Lei 8.666/93.

13.2. Havendo sanção punitiva, todos os pagamentos serão suspensos até comprovação do pagamento da multa ou justificativa que a abone.

13.3. A CONTRATADA incorrerá em multa de até 10% (dez por cento) sobre o valor total do contrato, sem prejuízo de outras sanções previstas no artigo 87 da Lei 8666/93, na hipótese de recusa injustificada pela licitante vencedora em aceitar ou receber as solicitações de serviço ou por descumprimento injustificado das cláusulas do edital;

13.3.1. Multa, na hipótese de atraso, no percentual correspondente a 1% (um por cento) calculado sobre o valor mensal, por dia de inadimplência, até o limite de 05 (cinco) dias, após este prazo será cobrada multa até 10% calculada sobre o valor total do contrato, caracterizando inexecução parcial do contrato (conforme a gravidade do caso);

13.4. A notificação da multa inicia o prazo para recurso, e à CONTRATANTE é facultado, caso a justificativa da CONTRATADA não seja aceita, descontar o valor da fatura a ser apresentada.

13.5. O valor da multa, aplicada após o regular processo administrativo, será deduzida da garantia ou, em sua insuficiência, das faturas devidas, ou ainda, cobradas diretamente da CONTRATADA, amigável ou judicialmente, na forma dos parágrafos 2º e 3º do artigo 86 da Lei nº 8.666/93, sendo a CONTRATADA notificada para recompor o valor inicial da garantia.

13.6. As sanções previstas poderão ser registradas em sistemas de cadastramento de fornecedores.

CLÁUSULA DÉCIMA QUARTA - DA RESCISÃO

14.1. O presente Contrato poderá ser rescindido por ato unilateral do CONTRATANTE, ou pela inexecução total ou parcial do presente contrato, com as consequências contratuais e as previstas nos artigos 77 e seguintes e 86 e seguintes todos da Lei nº 8.666/93 sem prejuízo das demais cominações previstas em outras normativas correlatas vigentes.

CLÁUSULA DÉCIMA QUINTA - DOS CASOS OMISSOS

15.1. Os casos omissos decorrentes da execução do presente Contrato serão resolvidos de comum acordo entre as partes, em último caso, remetido à autoridade superior da Administração do CONTRATANTE, para decidir, tudo em estrita observância à Lei nº 8.666/93.

CLÁUSULA DÉCIMA SEXTA – DOS CRITÉRIOS DE SUSTENTABILIDADE DO EDITAL

16.1. Os serviços serão prestados de acordo com os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão – SLTI/MPOG e no Decreto nº 7.746/2012, da Casa Civil, da Presidência da República, no que couber.

CLÁUSULA DÉCIMA SÉTIMA - DO FORO

20.1. Quaisquer dúvidas ou questões oriundas da execução do presente Contrato, que não forem passíveis de solução amigável, serão dirimidas em Juízo do Foro da Justiça Federal, Seção Judiciária do Rio de Janeiro.

E por estarem acordadas, assinam o presente em 02 (duas) vias de igual teor e forma na presença de 02 (duas) testemunhas.

Rio de Janeiro, ____ de _____ de 2018.

_____
CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO DE JANEIRO
CONTRATANTE

_____
CONTRATADO

TESTEMUNHAS:

1) Nome_____
CPF/MF n.:_____

2) Nome: _____
CPF/MF n: _____