



## EDITAL

### PREGÃO PRESENCIAL – SRP Nº 020/2017

#### 1. INTRODUÇÃO

**1.1. O CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO – COREN/RJ**, com sede na Avenida Presidente Vargas, nº 502, 5º andar, Centro, Rio de Janeiro/RJ, torna público que fará realizar licitação, sob a modalidade de **PREGÃO PRESENCIAL PARA REGISTRO DE PREÇOS - SRP**, do tipo **MENOR PREÇO POR LOTE**, para aquisição parcelada por registro de preços **Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o Coren-RJ e suas subseções, compreendendo o fornecimento, a implantação, o suporte técnico, a garantia e o treinamento do: Firewall de Borda no modo Cluster Ativo/Passivo – TIPO A, Sistema de Firewall Interno com Gerenciamento Centralizado (Stand Alone) – TIPO B, os dois firewalls deverão suportar Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall), Ponto de Acesso de Comunicação para Redes sem Fio e Switch PoE, conforme especificações constantes do Termo de Referência (Anexo I).**

**1.2.** O presente Pregão e a adjudicação dele decorrente se regem por toda a legislação aplicável à espécie, especialmente pelas normas de caráter geral da Lei Federal nº 10.520/2000 e Decreto Federal nº. 3.555 de 08 de agosto de 2000, no que couber, pelas normas da Lei Federal nº 8.666/93 e suas alterações, pelas Leis Complementares Federais nº 101/2000 (Lei de Responsabilidade Fiscal) e n.º 123/2006 (Estatuto Nacional da Microempresa e Empresa de Pequeno Porte), Lei Complementar nº 147/2014, em especial o Decreto nº 7892/2013, bem como pelas disposições constantes deste edital e seus anexos, normas que as licitantes declaram conhecer e a elas se sujeitam incondicional e irrestritamente.

**1.3.** O edital se encontra disponível no endereço eletrônico ([www.coren-rj.org.br](http://www.coren-rj.org.br)), no menu “Institucional”, submenu “Licitações”.

**1.4.** Os interessados poderão solicitar esclarecimentos acerca do objeto deste edital ou impugnar o ato convocatório deste pregão, até 02 (dois) dias úteis anteriores à data da licitação, no seguinte endereço: Avenida Presidente Vargas, nº 502, 6º andar, Centro, Rio de Janeiro, na sala do Setor de Compras e Suprimentos, de 10 (dez) até 16 (dezesesseis) horas, ou ainda, pelo e-mail: [pregao@coren-rj.org.br](mailto:pregao@coren-rj.org.br).



**1.5.** Caberá ao Pregoeiro decidir sobre a impugnação e pedidos de esclarecimentos no prazo de até 01 (um) dia antes da realização da sessão, com publicação da resposta no endereço eletrônico do COREN/RJ ([www.coren-rj.org.br](http://www.coren-rj.org.br)) no menu “Institucional”, submenu “Licitações”.

**1.6.** As retificações deste edital, por iniciativa oficial ou provocada por eventuais impugnações, obrigarão a todas as licitantes e serão publicadas no endereço eletrônico do COREN/RJ ([www.coren-rj.org.br](http://www.coren-rj.org.br)) no menu “Institucional”, submenu “Licitações”, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a modificação não alterar a formulação das propostas.

**1.7.** O Pregão a que se refere este edital poderá ser adiado, revogado por razões de interesse público decorrente de fato superveniente devidamente comprovado, ou anulado, sem que caiba às licitantes qualquer direito a reclamação ou indenização por estes motivos, nos termos do artigo 49 da Lei Federal n.º 8.666/93.

## **2. DO SISTEMA REGISTRO DE PREÇOS**

**2.1.** A presente licitação visa o registro de preços para eventual aquisição parcelada de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o Coren-RJ e suas subseções, compreendendo o fornecimento, a implantação, o suporte técnico, a garantia e o treinamento do: Firewall de Borda no modo Cluster Ativo/Passivo – TIPO A, Sistema de Firewall Interno com Gerenciamento Centralizado (Stand Alone) – TIPO B, os dois firewalls deverão suportar Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall), Ponto de Acesso de Comunicação para Redes sem Fio e Switch PoE, conforme especificações constantes dos Anexos do Termo de Referência.

**2.2.** A quantidade mínima a ser proposta deve atender ao menos à previsão de consumo do COREN/RJ, não sendo admitida cotação inferior.

**2.3.** Findo o processo licitatório, a Administração não terá obrigatoriedade em contratar.

**2.4.** Os preços permanecerão registrados pelo prazo de 12 (doze) meses. É vedado acréscimos nos quantitativos, conforme Art. 12, § 1º do Decreto 7892/2013.

**2.5.** A Ata de Registro de preços, durante sua vigência, somente poderá ser utilizada por órgão ou entidade da Administração que não tenha participado do certame licitatório, mediante prévia consulta e expressa autorização do COREN/RJ, nos termos do artigo 22, §4º do Decreto nº 7.892/13.



**2.6.** Não existem Órgãos Participantes previamente cadastrados junto ao COREN/RJ.

**2.7.** Não serão admitidas adesões ao presente registro de preços.

**2.8.** Em conformidade com Art. 9º, XI do Decreto nº 7892/2013, a Administração reserva-se o direito de realizar periodicamente pesquisa de mercado para comprovação da vantajosidade da Ata de Registro de Preços.

### **3. DIA, HORÁRIO E LOCAL DA ABERTURA DA LICITAÇÃO.**

**3.1.** No dia **06 de julho de 2017, às 11 horas**, o Pregoeiro e a Equipe de Apoio estarão reunidos na Sala de Reuniões na Av. Presidente Vargas n.º 502, 5º andar, na Cidade do Rio de Janeiro, para receber e iniciar a abertura dos envelopes referentes ao presente Pregão.

**3.2.** No caso da licitação não puder ser realizada na data estabelecida, será publicado, na página eletrônica do COREN/RJ, novo aviso de licitação indicando data, horário e endereço do local da sessão do Pregão.

### **4. DO OBJETO**

**4.1.** A presente licitação tem por objetivo o registro de preços pelo período de 12 (doze) meses, na forma do item 1.1 do edital e do **Anexo I**, que é parte integrante deste edital.

**4.2.** A quantidade indicada no **Anexo I** representa estimativa de consumo médio anual do Almoxarifado do Conselho Regional de Enfermagem do Rio de Janeiro, sem que haja obrigação de aquisição total durante toda a sua vigência.

### **5. RECURSOS ORÇAMENTÁRIOS**

**5.1.** Conforme entendimento do Tribunal de Contas da União (Acórdão TCU 3.146/2004 – Primeira Câmara e 1.279/2008 – Plenário), bem como do Art. 7º, § 2º do Decreto 7.892/2013 a indicação da dotação orçamentária é exigível apenas para a formalização do contrato ou outro instrumento hábil.

**5.2.** O valor total estimado desta licitação é de **R\$ 402.255,87** (quatrocentos e dois mil, duzentos e cinquenta e cinco reais e oitenta e sete centavos).

### **6. TIPO DE LICITAÇÃO**



**6.1.** O presente Pregão Presencial Para Registro de Preços - SRP é do tipo **MENOR PREÇO POR LOTE**, estando a descrição dos materiais, especificações, quantitativos por item e valores de referência contidos no **Anexo III**.

## **7. CONDIÇÕES DE PARTICIPAÇÃO**

**7.1.** Poderão participar do certame as pessoas jurídicas que atuem em ramo de atividade compatível com o objeto licitado.

**7.2.** Não serão admitidas neste Pregão as empresas suspensas do direito de licitar, no prazo e nas condições do impedimento, pela Administração Direta ou Indireta, inclusive Fundações, no nível federal, estadual e municipal e as declaradas inidôneas pela Administração Direta ou Indireta, inclusive Fundações, no nível federal, estadual e municipal bem como as que estiverem em regime de recuperação judicial ou extrajudicial.

**7.3.** Não será permitida a participação de mais de uma empresa sob o controle acionário de um mesmo grupo de pessoas físicas ou jurídicas.

**7.4.** Não será permitida a participação de licitantes cujos dirigentes, gerentes, sócios ou componentes do seu quadro técnico sejam servidores do COREN/RJ, ou que o tenham sido nos últimos 180 (cento e oitenta) dias anteriores à data deste edital, em consonância com o disposto no artigo 9º, inciso III, da Lei Federal n.º 8.666/93.

**7.5.** Não será permitida a participação de licitantes que tenham participado da elaboração do **Anexo I** como autores ou colaboradores, bem como de licitantes cujo quadro técnico seja integrado por profissional que tenha participado como autor ou colaborador do **Anexo I**.

**7.6.** Não será permitida a participação na licitação de empresas que estejam reunidas em consórcio ou coligação, ou de cooperativas.

**7.7.** Não será permitida a participação na licitação das pessoas físicas e jurídicas arroladas no artigo 9º da Lei n.º 8.666/93.

## **8. CREDENCIAMENTO**

**8.1.** Na data, horário e local indicados no item **3.1** deste edital, as empresas interessadas deverão se credenciar junto ao Pregoeiro.



**8.2.** As empresas participantes serão representadas na sessão do Pregão por seu representante legal, que deverá estar devidamente munido de credencial que o autorize a participar do procedimento licitatório.

**8.3.** Por credencial entende-se:

a) Procuração passada por instrumento público ou particular, com firma reconhecida em cartório, que contenha poderes “*ad judícia*” e “*ad negocia*” para formulação de proposta e lances de preços, manifestar a intenção de recorrer e de desistir dos recursos, bem como praticar todos os demais atos pertinentes ao certame, em nome da empresa licitante ou declaração na forma do **Anexo II (carta de credenciamento)**, em ambos os casos, acompanhada dos atos constitutivos da empresa;

b) Documento comprobatório de capacidade para representar a empresa, no qual estejam expressos seus poderes para exercer direitos e assumir obrigações em decorrência de tal investidura, no caso de sócio ou dirigente da mesma.

**8.4.** O representante deverá, antes da entrega dos envelopes e da credencial, identificar-se exibindo a Carteira de Identidade ou outro documento equivalente, em original, **acompanhada de uma cópia.**

**8.5.** A proponente deverá apresentar ao Pregoeiro, **de forma avulsa,** Declaração de Pleno Atendimento aos Requisitos de Habilitação, dando ciência de que cumpre plenamente os requisitos de habilitação, nos termos do inciso VII, artigo 4º, da Lei nº 10.520/2002 (**Anexo V**).

**8.6. A não apresentação da declaração prevista no subitem 8.5 ou da credencial descrita no subitem 8.3 implicará a desclassificação imediata da licitante, resultando o mesmo efeito no caso de incorreção desses documentos.**

## **9. CREDECIAMENTO DAS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE**

**9.1.** A microempresa ou empresa de pequeno porte deverá respeitar todo o disposto no **item 8** deste edital.

**9.2.** Além disso, a microempresa e empresa de pequeno porte que optar pela fruição dos benefícios estabelecidos na Lei Complementar nº 123/2006 deverá apresentar comprovante de opção pelo SIMPLES NACIONAL ou Declaração firmada pela licitante, na forma do (Anexo IV), **sob pena de não o fazendo no ato de credenciamento,** renunciar ao direito de participar do Pregão como microempresa ou empresa de pequeno porte.

## **10. APRESENTAÇÃO DAS PROPOSTAS DE PREÇO E DA DOCUMENTAÇÃO**



**10.1.** Declarados encerrados os procedimentos de credenciamento, não mais serão admitidos novos proponentes, dando-se início ao recebimento dos envelopes de proposta de preço e documentação.

**10.2.** Os documentos e as propostas exigidos no presente edital serão apresentados em 02 (dois) envelopes indevassáveis e lacrados, constando obrigatoriamente da parte externa de cada um as seguintes indicações:

**ENVELOPE “A” - PROPOSTA DE PREÇO - 01 (uma) via**

**“CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO –COREN/RJ”**

**PREGÃO PRESENCIAL- SRP N° /2017**

**NOME COMPLETO E ENDEREÇO DA LICITANTE**

**ENVELOPE “B” - DOCUMENTAÇÃO DE HABILITAÇÃO - 01 (uma) via**

**“CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO – COREN/RJ”**

**PREGÃO PRESENCIAL- SRP N° /2017**

**NOME COMPLETO E ENDEREÇO DA LICITANTE**

## **11. FORMA DE APRESENTAÇÃO DAS PROPOSTAS E DOS DOCUMENTOS**

**11.1.** Os documentos dos envelopes "A" - PROPOSTA DE PREÇO e "B" - HABILITAÇÃO serão apresentados na forma estabelecida nos itens abaixo.

**11.2.** O ENVELOPE "A" - PROPOSTA DE PREÇO - deverá conter o formulário PROPOSTA DE PREÇO em 01 (uma) via, de acordo com o modelo fornecido pelo Conselho Regional de Enfermagem do Rio de Janeiro e que integra o presente edital (**Anexo IV**), devidamente preenchido e elaborado pela licitante, carimbado com o sinal/símbolo da licitante e assinado pelos seus representantes legais.

**11.3.** Os valores unitário e global serão apresentados em algarismos, com duas casas decimais, sem rasuras ou entrelinhas, e por extenso, prevalecendo, em caso de discrepância, o valor por extenso. No caso de números inteiros, será dispensável a apresentação do algarismo zero nas casas decimais.

**11.4.** Os preços propostos são fixos e irajustáveis e incluem todas as despesas necessárias para o fornecimento e entrega dos produtos nas condições do presente edital, incluindo todos os custos diretos e indiretos, taxas, remuneração, despesas fiscais e financeiras, e quaisquer despesas extras e necessárias



não especificadas neste edital, mas julgadas essenciais ao cumprimento do objeto deste Pregão. Nenhuma reivindicação para pagamento adicional será considerada se decorrer de erro ou má interpretação do objeto deste edital.

**11.5. Não serão admitidas, sob quaisquer motivos, modificações ou substituições da proposta ou de quaisquer documentos, uma vez entregues os envelopes indicados no subitem 10.2.**

**11.6.** As licitantes arcarão com todos os custos relativos à apresentação das suas propostas. O COREN/RJ, em nenhuma hipótese, será responsável por tais custos, quaisquer que sejam os procedimentos seguidos no Pregão Presencial- SRP ou os seus resultados.

**11.7.** O ENVELOPE “B” – HABILITAÇÃO - deverá conter os documentos especificados a seguir:

- (A) - Documentação relativa à habilitação jurídica;
- (B) - Documentação relativa à qualificação econômico-financeira;
- (C) - Documentação relativa à regularidade fiscal;
- (D) - Documentação relativa à regularidade trabalhista;
- (E) - Documentação relativa à qualificação técnica;
- (F) - Outros documentos.

**(A) - DOCUMENTAÇÃO RELATIVA À HABILITAÇÃO JURÍDICA**

(A.1) - Registro Comercial, no caso de empresa individual.

(A.2) - Estatuto ou Contrato Social em vigor, devidamente registrado, em se tratando de sociedades comerciais e, no caso de sociedade por ações, acompanhados de documentos de eleição de seus administradores.

(A.3) - Inscrição do Ato Constitutivo, no caso de sociedade civil, acompanhada da prova da composição da diretoria em exercício.

(A.4) - 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.

**(A.5) - Na hipótese de existir alteração nos documentos citados nos subitens (A.2) e (A.3), posteriormente à constituição da firma ou da sociedade, os referidos documentos deverão ser apresentados de forma consolidada, contendo todas as cláusulas em vigor.**

**(B) - QUALIFICAÇÃO ECONÔMICO-FINANCEIRA**



**(B.1)** - Comprovação de ser dotada de capital social devidamente integralizado ou de patrimônio líquido igual ou superior a 10% (dez por cento) do valor estimado para a contratação. A comprovação será obrigatoriamente feita pelo Ato Constitutivo, Estatuto ou Contrato Social em vigor e devidamente registrado **ou** pelo balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, conforme disposto no artigo 31, inciso I, da Lei Federal n° 8.666/93.

**(B.2)** - Certidões negativas de recuperação judicial ou concordata expedidas pelo Distribuidor da sede da licitante. Para as licitantes sediadas na Cidade do Rio de Janeiro, a prova será feita mediante apresentação de certidões dos 1º, 2º, 3º e 4º Ofícios de Registro de Distribuição. **As licitantes sediadas em outras comarcas do Estado do Rio de Janeiro ou em outros Estados deverão apresentar, juntamente com as certidões negativas exigidas, declaração passada pelo foro de sua sede, indicando quais os Cartórios ou Ofícios de Registros que controlam a distribuição de falências, recuperação judicial e extrajudicial e concordata.**

### **(C) - DOCUMENTAÇÃO RELATIVA À REGULARIDADE FISCAL**

**(C.1)** - Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda (CNPJ).

**(C.2)** - Prova de inscrição no cadastro de contribuintes estadual ou municipal, se houver, relativo ao domicílio ou sede da licitante, pertinente ao objeto deste Pregão.

**(C.3)** - Prova de regularidade perante as Fazendas Nacional, Estadual e Municipal do domicílio ou sede do licitante com a apresentação das seguintes certidões:

**(C.3.a)** - A prova de regularidade com a Fazenda Federal será efetuada por meio da certidão conjunta negativa de débitos (ou positiva com efeitos de negativa) relativos a tributos federais e à dívida ativa da União, ou certidão conjunta positiva com efeitos de negativa, expedida pela Secretaria da Receita Federal do Brasil e Procuradoria Geral da Fazenda Nacional, da sede da licitante.

**(C.3.a.1)** - Certidão negativa de débito ou certidão positiva com efeitos de negativa referente à Contribuição Previdenciária e às de Terceiros, expedida pela Secretaria da Receita Federal do Brasil, da sede do licitante. **As certidões antes emitidas pelo Instituto Nacional do Seguro Social são atualmente emitidas pela Secretaria da Receita Federal do Brasil, sendo exceção somente o caso de Contribuinte Individual.**

**(C.3.b)** - Prova de regularidade com a Fazenda Estadual, por meio de apresentação da respectiva certidão negativa de débito (ou positiva com efeitos de negativa), ou, se for o caso, certidão comprobatória de que a licitante, pelo respectivo objeto, está isenta de inscrição estadual;



**(C.3.b.1)** - Caso a licitante seja estabelecida no Estado do Rio de Janeiro, a prova de regularidade com a Fazenda Estadual será feita por meio de apresentação da certidão negativa ou positiva com efeitos de negativa de imposto sobre a circulação de mercadorias e serviços expedida pela Secretaria Estadual da Fazenda e certidão de dívida ativa para fins de licitação expedida pela Procuradoria Geral do Estado, ou, se for o caso, certidão comprobatória de que a licitante, pelo respectivo objeto, está isenta de inscrição estadual;

**(C.3.c)** - A prova de regularidade com a Fazenda Municipal será feita por meio da certidão negativa ou positiva com efeitos de negativa de imposto sobre serviços de qualquer natureza, ou, se for o caso, certidão comprobatória de que a licitante, pelo respectivo objeto, está isenta de inscrição Municipal.

**(C.4)** - Prova de regularidade perante o Fundo de Garantia por Tempo de Serviço (FGTS).

**(C.5)** - Certidão Negativa de Débitos Trabalhista (**CNDT**), para comprovar a inexistência de débitos inadimplidos perante a Justiça do Trabalho.

#### **(D) - DOCUMENTAÇÃO RELATIVA À REGULARIDADE TRABALHISTA**

**(D.1)** - Declaração, na forma do **Anexo VI**, de que não possuem em seus quadros funcionários menores de 18 (dezoito) anos desempenhando trabalho noturno, perigoso ou insalubre ou funcionários menores de 16 (dezesesseis anos), na forma do art. 7º, inciso XXXIII, da Constituição Federal.

#### **(E) – DOCUMENTAÇÃO RELATIVA À QUALIFICAÇÃO TÉCNICA**

**(E.1)** - Comprovação de aptidão das licitantes para desempenho de atividade pertinente e compatível com o objeto da licitação, por meio de certidões ou atestados, fornecidos por pessoa jurídica de direito público ou privado, atestado que a licitante prestou satisfatoriamente serviços compatíveis com o objeto desta licitação;

#### **(F) - OUTROS DOCUMENTOS**

**(F.1)** - Declaração de compromisso e idoneidade, conforme **Anexo VII**, elaborada em papel timbrado e subscrita pelo representante legal da licitante, assegurando a inexistência de impedimento legal para licitar ou contratar com a Administração Pública.

### **12. DA HABILITAÇÃO DAS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE**

**12.1.** A microempresa e empresa de pequeno porte, beneficiárias do regime diferenciado instituído pela Lei Complementar nº 123/2006 e Lei Complementar nº 147/2014, após a etapa de lances, deverá apresentar toda a documentação exigida para habilitação, inclusive aquela que comprova sua regularidade fiscal, mesmo que apresente alguma restrição.



**12.2. Caso a documentação apresentada pela microempresa ou pela empresa de pequeno porte contenha alguma restrição, lhe será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento que a empresa for declarada vencedora do certame, ou após o julgamento de eventuais recursos, prorrogáveis por igual período, a critério da Administração Pública, para a regularização da documentação.**

12.3. A não regularização da documentação no prazo estipulado implicará a decadência do direito à contratação, sem prejuízo da aplicação das sanções previstas no artigo 81 da Lei nº 8.666/93.

### **13. DA SESSÃO DO PREGÃO**

#### **13.1. DA ABERTURA DAS PROPOSTAS DE PREÇO**

13.1.1. Após a fase de credenciamento, o Pregoeiro procederá à abertura dos envelopes com as propostas de preços, verificando a conformidade das propostas com os requisitos estabelecidos neste edital, desclassificando, preliminarmente, aquelas que estiverem em desacordo com o edital.

13.1.2. Verificada a compatibilidade com o exigido no edital será classificada a proposta de menor preço por item e aquelas que tenham valores sucessivos e superiores em até 10% (dez por cento) daquela.

13.1.3. Quando não existirem no mínimo 03 (três) propostas sucessivas e superiores em até 10% (dez por cento) da menor proposta de preço por item, serão classificadas as três melhores propostas, já incluída a da licitante que tiver apresentado o menor preço na proposta escrita.

13.1.4. Havendo empate entre propostas de preço por item que se enquadrem nas hipóteses escritas nos dois subitens anteriores, serão todas classificadas, realizando-se sorteio para determinação da ordem de oferta dos lances.

#### **13.2. DOS LANCES VERBAIS**

13.2.1. Após a classificação das propostas, o Pregoeiro as divulgará em voz alta, e convidará, individualmente, os representantes das licitantes classificadas a apresentarem lances verbais, a partir da proposta classificada de maior preço por item, seguido dos demais, de forma sucessiva e em valores distintos e decrescentes.

13.2.2. O Pregoeiro poderá estipular redução mínima entre os lances.

13.2.3. A desistência em apresentar lance verbal, quando for feita a convocação pelo Pregoeiro, importará a exclusão da licitante da etapa de apresentação de lances verbais, com a manutenção do



último preço por ela apresentado para efeito de ordenação das propostas. Caso todas as licitantes se recusarem a apresentar lances verbais, a ordem de classificação das propostas escritas será mantida.

**13.2.4.** A rodada de lances verbais será repetida quantas vezes o Pregoeiro considerar necessário.

**13.2.5.** O Pregoeiro poderá, motivadamente, estabelecer limite de tempo ou o uso de telefone celular para a fase de formulação dos lances verbais, mediante prévia comunicação às licitantes.

**13.2.6. Não serão aceitos dois ou mais lances do mesmo valor, prevalecendo aquele que for recebido em primeiro lugar.**

**13.2.7.** Declarada encerrada a etapa competitiva, as propostas serão reordenadas e o Pregoeiro examinará a aceitabilidade da primeira classificada quanto ao objeto e valor, decidindo motivadamente.

**13.2.8.** Para julgamento e classificação das propostas, será adotado o critério de menor preço por item, observado as exigências estabelecidas no **Anexo I** do edital.

**13.2.9.** Os preços ofertados após a etapa de lances não poderão ser superiores aos preços de mercado, levantados pela Administração como critério de aceitabilidade.

**13.2.10.** Caso a melhor oferta tenha sido formulada por microempresa ou empresa de pequeno porte, o pregoeiro iniciará a etapa de negociação.

**14.2.11.** Quando a melhor oferta tenha sido formulada por licitante que não seja micro empresa ou empresa de pequeno porte, o Pregoeiro deverá verificar a existência de empate ficto, nos termos do **artigo 44, § 2º da Lei Complementar nº 123/2006**, e, em caso positivo, proceder ao desempate segundo as regras a seguir estabelecidas:

**13.2.11.1.** Entende-se por empate ficto aquelas situações em que as propostas apresentadas por microempresas ou empresas de pequeno porte sejam iguais ou até 5% (cinco por cento) superiores à proposta mais bem classificada;

**13.2.11.2.** Havendo empate ficto, proceder-se-á da seguinte forma:

**a)** a microempresa ou empresa de pequeno porte mais bem classificada será convocada para apresentar proposta de preço inferior àquela vencedora do certame no prazo máximo de 05 (cinco) minutos, após o encerramento da fase de lances, sob pena de preclusão;

**b)** caso a microempresa ou empresa de pequeno porte, que se apresente neste caso, abdique desse direito, serão convocadas, na ordem classificatória, as demais que se enquadrem na mesma hipótese, para o exercício de igual direito;



c) na situação de empate na forma antes prevista, inexistindo oferta de lances e existindo equivalência nos valores apresentados por mais de uma microempresa ou empresa de pequeno porte, a ordem para formulação de nova proposta será estabelecida por sorteio.

**13.2.12.** Caso não haja empate ficto, o Pregoeiro iniciará a fase de negociação com a empresa originalmente vencedora do certame.

**13.2.13.** Se a proposta ou o lance de menor valor não for aceitável, o Pregoeiro examinará a proposta ou o lance subsequente, na ordem de classificação, verificando a sua aceitabilidade. Se for necessário, repetirá esse procedimento, sucessivamente, até a apuração de uma proposta ou lance que atenda ao edital.

**13.2.14.** Sendo aceitável a proposta de menor preço por item, será aberto o envelope contendo a documentação de habilitação da licitante que a tiver formulado, para confirmação das suas condições habilitatórias.

#### **14. DA FASE DE HABILITAÇÃO**

**14.1.** Os documentos exigidos no ENVELOPE "B" - HABILITAÇÃO - poderão ser apresentados no original ou em cópia reprográfica autenticada, na forma do artigo 32 da Lei Federal nº 8.666/93 e rubricados pelo representante legal da licitante, e acompanhados das respectivas certidões de publicação no órgão da imprensa oficial, quando for o caso.

**14.2. As folhas da documentação serão numeradas em ordem crescente e não poderão conter rasuras ou entrelinhas.** Na hipótese de falta de numeração, numeração equivocada ou ainda inexistência de rubrica do representante legal na documentação, poderá o Pregoeiro solicitar ao representante da firma, devidamente identificado e que tenha poderes para tanto, que, durante a sessão de abertura do envelope "B", sane a incorreção.

**14.3.** No caso de autenticação de cópia reprográfica por servidor da Administração, o mesmo deverá integrar a Equipe de Apoio ou ser o Pregoeiro, devendo os documentos ser apresentados e autenticados no momento da abertura dos envelopes.

**14.4. Se os Certificados, declarações, registros e certidões não tiverem prazo de validade declarado no próprio documento, da mesma forma que não conste previsão em legislação específica, os referidos documentos deverão ter sido emitidos há, no máximo, 90 (noventa) dias, contados até a data da realização da licitação.**



14.5. Os documentos exigidos para habilitação não poderão, em hipótese alguma, ser substituídos por protocolos que apenas comprovem o seu requerimento.

14.6. O Pregoeiro poderá pedir, a qualquer tempo, a exibição do original dos documentos.

**14.7. Se a primeira colocada não for considerada habilitada, o Pregoeiro examinará a oferta subsequente, realizando negociação, verificando sua aceitabilidade e precedendo à habilitação do proponente, na ordem de classificação, e assim sucessivamente.**

14.8. Da sessão lavrar-se-á ata circunstanciada, contendo, sem prejuízo de outros, o registro das licitantes credenciadas, das propostas escritas e verbais apresentadas, na ordem de classificação, da análise da documentação exigida para a habilitação e dos recursos interpostos e que, ao final, será assinada pelo Pregoeiro e demais membros da Equipe de Apoio, bem como pelas licitantes presentes.

## 15. DOS RECURSOS

15.1. Ao final da sessão e declarada a vencedora do certame pelo Pregoeiro, qualquer licitante poderá manifestar imediatamente e **motivadamente** a intenção de interpor recurso, quando lhe será concedido o prazo de 03 (três) dias para a apresentação das razões do recurso, ficando as demais licitantes, **desde logo, intimadas para apresentar contrarrazões** em igual número de dias, que começarão a correr do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos autos.

15.2. A não apresentação das razões escritas acarretará, como consequência, a análise do recurso pela síntese das razões orais.

**15.3. A falta de manifestação imediata e motivada da licitante acarretará decadência do direito de recurso e a adjudicação do objeto da licitação pelo Pregoeiro ao vencedor.**

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

15.5. Os recursos serão dirigidos ao Pregoeiro, que poderá reconsiderar seu ato, no prazo de 03 (três) dias úteis, ou então, neste mesmo prazo, encaminhar o recurso, devidamente instruído à autoridade superior, que proferirá a decisão no prazo de 03 (três) dias úteis, a contar do seu recebimento.

## 16. DA ATA DE REGISTRO DE PREÇOS

16.1. Homologado o certame, os vencedores serão convocados por qualquer meio hábil que se possa comprovar o recebimento da convocação, aceitando-se inclusive os meios eletrônicos: e-mail, fac-símile entre outros, visando à entrega da Proposta Comercial adequada ao lance vencedor e a assinatura da Ata



de Registro de Preços, conforme **Anexo IX**, no prazo de até 3 (três) dias úteis contados do recebimento da notificação, sob pena de incidir na infração do artigo 81 da Lei n° 8.666/93.

**16.2.** Não haverá obrigatoriedade da Administração contratar, podendo, inclusive, realizar outro procedimento licitatório para aquisição do mesmo objeto, nos termos do Art. 16 do Decreto 7892/13, respeitando-se a preferência ao beneficiário do registro, em igualdade de condições, nos termos do artigo 15, § 4° da Lei 8.666/93.

**16.3.** A Ata de Registro de Preços terá vigência de 12 (doze) meses, permanecendo fixo e irrevogável o preço registrado.

**16.4.** A Administração deverá promover as necessárias negociações junto aos fornecedores no caso de pedido de redução ou elevação dos preços registrados.

## **17. CANCELAMENTO DO REGISTRO DE PREÇOS**

**17.1.** Assegurados o contraditório e a ampla defesa, o fornecedor do bem terá seu Registro de Preços cancelado quando:

**I** - descumprir as condições da Ata de Registro de Preços;

**II** - recusar-se a celebrar o contrato ou não retirar o instrumento equivalente, no prazo estabelecido pela Administração, sem justificativa aceitável;

**III** - não aceitar reduzir seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

**17.1.1.** Independentemente das previsões retro indicadas, o fornecedor do bem poderá solicitar o cancelamento de seu Registro de Preço na ocorrência de fato superveniente que venha comprometer a perfeita execução contratual, decorrente de caso fortuito ou de força maior devidamente comprovado.

## **18. DA ENTREGA E RECEBIMENTO**

**18.1.** A licitante deverá entregar o material requisitado na forma prevista no Termo de Referência (**Anexo I**), parte integrante deste edital.

**18.2.** Os produtos deverão ser entregues acondicionados adequadamente e estar acompanhado da nota fiscal correspondente, devidamente preenchida.

**18.3.** O objeto será recebido na forma prevista no Art. 73, da Lei n° 8.666/93, dispensado o recebimento provisório nas hipóteses previstas no Art. 74 da mesma Lei.



**18.4.** O recebimento provisório ou definitivo do objeto não exclui a responsabilidade civil a ele relativa, nem a ético-profissional, pela sua perfeita execução.

**18.5.** O fornecedor é inteiramente responsável pela entrega. Não será fornecido equipamento ou mão-de-obra para que o material seja transportado até o setor de Almoxarifado

**18.6.** Após o prazo de 05 (cinco) dias úteis, verificada compatibilidade do material com o edital e proposta, será recebido definitivamente, emitindo-se o Termo de Recebimento Definitivo, conforme **Anexo VIII**.

**18.7.** Constatadas irregularidades, a Administração poderá:

**18.7.1.** No que diz respeito à especificação, rejeitá-lo no todo ou em parte, determinando sua substituição ou complementação, ou rescindindo a contratação, sem prejuízo das penalidades cabíveis.

**18.7.2.** Na hipótese de substituição, a licitante deverá fazê-la em conformidade com a indicação da Administração, no prazo máximo de 03 (três) dias úteis contados da notificação por escrito, mantidos os preços inicialmente registrados.

**18.7.3.** Na hipótese do subitem anterior, o prazo previsto no subitem **20.2** será interrompido até que sejam sanadas as irregularidades, recomeçando seu cômputo apenas quando da efetivação da nova entrega dos materiais substituídos ou complementados.

**18.7.4.** A entrega do material substituído ou complementado dar-se-á novamente de forma provisória, a fim de que seja novamente aferida a sua compatibilidade com os termos do presente edital.

**18.7.5.** Verificando-se que a nova entrega está em termos, será emitido Termo de Recebimento Definitivo.

**18.7.6.** Caso a nova entrega ainda se verifique fora dos padrões do edital, a Administração optará entre notificar novamente a detentora ou declarar o inadimplemento contratual, com a aplicação das sanções pertinentes.

## **19. DA FORMA DE PAGAMENTO**

**19.1.** Para efeito de pagamento, prevalece a oferta obtida na data da licitação, observando-se a regular liquidação da despesa, nos termos do artigo 63 da Lei Federal nº 4.320/64, obedecido ao disposto no artigo 71 da Lei Federal nº 8.666/93.



**19.2.** O pagamento será efetuado após a entrega dos produtos, por intermédio de crédito em conta corrente da licitante vencedora, em até 30 (trinta) dia subsequente ao **RECEBIMENTO DEFINITIVO** do mesmo, sempre de acordo com a ordem cronológica de sua exigibilidade.

**19.3.** O COREN/RJ efetuará retenção na fonte de todos os tributos inerentes à prestação do serviço em questão.

**19.4.** Em caso de atraso no pagamento, o débito será acrescido da taxa de 1% (um por cento) ao mês, calculada *pro rata die* entre o 31º dia da data do adimplemento da obrigação e a data do efetivo pagamento.

**19.5.** O pagamento do valor global de cada solicitação se dará após a apresentação da fatura, que será aprovada e atestada pelo representante legal designado por este COREN/RJ, sendo também necessária a apresentação dos comprovantes de Certidão Negativa de Débito junto ao INSS (CND), Certificado de Regularidade junto ao FGTS e Certidão Negativa de Tributos Federais e Dívida Ativa da União.

**19.6.** O pagamento da fatura está condicionado à apresentação de Certidão Negativa de Débito junto ao INSS (CND), Certificado de Regularidade junto ao FGTS e Certidão Negativa de Tributos Federais e Dívida Ativa da União, sendo franqueado a contratante reter os pagamentos, rescindir o contrato, aplicar as demais sanções administrativas e promover a consignação judicial dos valores retidos acaso o contratado não regularize a sua situação fiscal no prazo de 20 (vinte) dias contados no recebimento de notificação expedida pela contratante para tanto.

## **20. DAS SANÇÕES ADMINISTRATIVAS**

**20.1.** Sem prejuízo de indenização por perdas e danos, cabível nos termos do Código Civil, a Administração poderá impor à licitante, adjudicatária ou contratada, pelo descumprimento total ou parcial das obrigações a que esteja sujeita, as sanções previstas no artigo 7º da Lei Federal nº 10.520/2002 e no artigo 87 da Lei nº 8.666/1993.

**20.2.** O atraso injustificado na entrega dos materiais sujeitará a Adjudicatária à multa demora, fixada neste edital.

**20.3.** Pela inexecução total ou parcial da obrigação assumida, a Administração poderá aplicar as seguintes sanções, garantida prévia defesa:

**20.3.1.** Advertência;

**20.3.2.** Multa de mora de até 1% (um por cento) por dia útil sobre o valor total dos itens, até o período máximo de 30 (trinta) dias úteis;



**20.3.3.** Multa de até 20% (vinte por cento) sobre o valor total dos itens, após esgotado o prazo fixado no subitem anterior;

**20.3.4.** Suspensão temporária de participação em licitação, ou impedimento de contratar com a Administração por prazo não superior a 02 (dois) anos;

**20.3.5.** Declaração de inidoneidade para licitar ou contratar com a Administração Pública, pelo prazo de até 05 (cinco) anos.

**20.4.** As sanções previstas nos subitens **20.3.1**, **20.3.4** e **20.3.5** poderão ser aplicadas juntamente com aquelas previstas em **20.3.2** e **20.3.3**, e não exclui a possibilidade de rescisão administrativa da avença, garantida defesa prévia ao interessado, no respectivo processo.

**20.5.** As sanções estabelecidas nos subitens **20.3.4** e **20.3.5** são da competência da Presidência do COREN/RJ.

**20.6.** As sanções previstas nos subitens **20.3.4** e **20.3.5** poderão também ser aplicadas às licitantes que, em outras contratações com a Administração Pública de qualquer nível federativo ou com autarquias, fundações, empresas públicas ou sociedade de economia mista tenham:

- a) sofrido condenação definitiva por praticarem, por meios dolosos, fraudes fiscais no recolhimento de quaisquer tributos;
- b) praticados atos ilícitos, visando a frustrar os objetivos da licitação;
- c) demonstrado não possuir idoneidade para contratar com a Administração, em virtude de outros atos ilícitos praticados.

## **21. DA VALIDADE DO REGISTRO DE PREÇOS**

**21.1.** O prazo de validade do Registro de Preços será de **12 (doze) meses**, contados a partir da data da publicação da respectiva Ata.

## **22. DO FORO**

**22.1.** Fica eleito o foro da Justiça Federal da Cidade do Rio de Janeiro para dirimir quaisquer questões, dúvidas ou demandas referentes à execução do objeto desta licitação e adjudicação dela decorrente.

## **23. DAS DISPOSIÇÕES FINAIS**



**23.1.** É facultada do Pregoeiro, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar originalmente da proposta ou da documentação.

**23.2.** Quando **todos os licitantes forem inabilitados ou todas as propostas forem desclassificadas**, o Pregoeiro poderá fixar aos licitantes o prazo de 08 (oito) dias úteis para a apresentação de nova documentação ou de outras propostas.

**23.3.** À adjudicatária caberá inteira responsabilidade por todos os encargos e despesas com salários de empregados, acidentes que possam vir a ser vítimas quando em serviço e por tudo assegurado nas leis sociais e trabalhistas, ficando responsável, outrossim, por quaisquer danos ou prejuízos causados a terceiros ou ao patrimônio do COREN/RJ por seus empregados.

**23.4.** Na entrega dos bens adquiridos deverão ser observadas, rigorosamente, as especificações preestabelecidas no **Anexo I**. Quando necessários, serão realizados testes e demais provas requeridas por normas técnicas oficiais, para a verificação da boa execução do objeto da presente licitação, correm à conta da licitante.

**23.5.** Na contagem dos prazos estabelecidos neste edital excluir-se-á o dia do início e incluir-se-á o do vencimento.

**23.6.** Ficam as licitantes sujeitas às sanções administrativas, cíveis e criminais cabíveis caso apresentem, na licitação, qualquer declaração falsa que não corresponda à realidade dos fatos.

**23.7.** A assinatura da **ATA DE REGISTRO DE PREÇOS** não implicará em direito à contratação.

**23.8.** Os casos omissos deste edital serão resolvidos pelo Pregoeiro.

**23.9.** Integram o presente Edital todas as instruções, observações e restrições contidas nos seus anexos:

Anexo I - Termo de Referência;

Anexo II - Carta de Credenciamento;

Anexo III - Modelo Proposta de Preços;

Anexo IV - Declaração para microempresa e empresa de pequeno porte;

Anexo V - Declaração referente à Habilitação;

Anexo VI - Declaração em atendimento ao artigo 27, inciso V, da Lei 8666/93 e artigo 7º, inciso XXXIII, da Constituição Federal;

Anexo VII - Declaração de cumprimento do artigo 32, § 2º, da Lei 8666/93;



**Coren<sup>RJ</sup>**  
Conselho Regional de Enfermagem do Rio de Janeiro

Processo nº: 1480/2016

Data: 05/12/2016

Folhas:

Rubrica:

Anexo VIII - Termo de Recebimento Definitivo;

Anexo IX - Minuta de Ata de Registro de Preços;

Anexo X - Modelo de Solicitação de Fornecimento;

Anexo XI - Descrição dos Materiais, Quantitativos e Valores de Referência

Anexo XII – Minuta do Contrato

**25.10.** Este Edital e seus Anexos contêm 82 (oitenta e duas) folhas.

Rio de Janeiro, 20 de junho de 2017

**MARCELO ALVES HENRIQUE PINTO MOREIRA**

Pregoeiro



## ANEXO I TERMO DE REFERÊNCIA

### 1. OBJETO

O presente termo de referência tem por objeto a Aquisição de Solução de Segurança da Informação e rede acesso sem fio, através da contratação de empresa especializada na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para a Sede do Coren-RJ e suas subseções, conforme especificações constantes nos Anexos deste presente Edital, compreendendo o fornecimento, a instalação, o suporte técnico, a garantia, o treinamento, o gerenciamento e o monitoramento de sistemas de: (i) Firewall do TIPO A – Firewall de Borda no modo Cluster Ativo/Passivo com suporte a Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall); (ii) Firewall do TIPO B – Firewall Interno com Gerenciamento Centralizado (Stand Alone) com suporte a Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall); (iii) Ponto de Acesso de Comunicação para Redes sem Fio; (iv) Switch PoE de Comunicação para Redes sem Fio de 24 portas (v) Switch de Comunicação para Redes de 48 portas.

A instalação e demais serviços aqui descritos serão prestados no território do CONTRATANTE, presencialmente no COREN/RJ, localizado à Avenida Presidente Vargas, nº 502, 3º, 4º, 5º e 6º Andares, Centro, Rio de Janeiro-RJ ou através de acesso remoto.

#### 1.1. OBJETIVO GERAL

O presente Termo de Referência visa municiar a CONTRATADA com Soluções de Segurança da Informação, Infraestrutura de rede e mão de obra especializada.

#### 1.2. OBJETIVO ESPECÍFICO

Prover o Coren-RJ com as seguintes soluções:

1.2.1 Firewall do TIPO A – Firewall de Borda no modo Cluster Ativo/Passivo com suporte a Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall),

1.2.2 Firewall do TIPO B – Firewall Interno com Gerenciamento Centralizado (Stand Alone) com suporte a Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall),

1.2.3 Ponto de Acesso de Comunicação para Redes sem Fio,

1.2.4 Suporte da Solução,

1.2.5 Implantação da Solução,

1.2.6 Treinamento da Solução,

1.2.7 Switch PoE e Comunicação para Redes sem Fio,

1.2.8 Switch PoE de Comunicação 24 portas para Redes sem Fio (vi) Switch de Comunicação 48 portas para Redes.

### 2. JUSTIFICATIVA

Considerando que o DTIC realiza o gerenciamento dos serviços de Internet, fazendo uso de uma solução de Firewall atualmente instalada em um servidor virtual, que viabiliza a filtragem dos conteúdos que são acessados internamente e promove a proteção da rede interna do Conselho contra acessos externos indevidos. Atualmente, o serviço realizado pela solução em uso foi descontinuado pelo fabricante – Microsoft e não possui suporte, logo não possui proteção contra ataques ou explorações de



vulnerabilidades provenientes e destinadas às redes internas, ou seja, todos os canais de comunicação do Coren-RJ têm acesso liberado entre si. Dessa forma, máquinas infectadas por códigos maliciosos em uma determinada unidade podem ser a causa de problemas em outras unidades, já que a ausência de inspeção do tráfego interno propicia este tipo de ocorrência.

O bom uso dos recursos de tecnologia da informação, principalmente no que tange à qualidade da navegação web das unidades do Coren-RJ é um dos principais fatores que nortearam a elaboração do presente projeto, pois os usuários possuem seus perfis identificados e tratados localmente, com liberações e restrições de acesso que os acompanham pelas estações de trabalho que estiverem utilizando. Uma política de liberação de acesso web mais adequado às necessidades institucionais que respeite as especificidades de cada unidade precisa se fazer presente.

O Coren-RJ vem ao longo dos últimos anos realizando investimentos significativos na informatização de suas atividades, fato que permitiu o tratamento do crescente volume de dados, gerado em decorrência do aumento considerável de tráfego em sua rede lógica, acrescido de variado conjunto de informações utilizado para as mais diversas finalidades. No entanto, para que tais informações funcionem efetivamente como ferramenta de trabalho para os usuários do Coren-RJ, é preciso assegurar que tais informações estejam disponíveis no momento em que forem necessárias e que tenham sua integridade e atualizações asseguradas com acompanhamento eficiente por parte dos administradores da rede.

Adicionalmente, deverá ser observado que o conjunto de informações hoje existente no âmbito do Coren-RJ constitui um importante patrimônio público, tornando-se, portanto, imprescindível a adoção de medidas para sua manutenção e preservação. À vista do exposto, é escopo do presente termo de referência delinear os requisitos dos serviços de segurança da informação a serem contratados, bem como especificá-los para garantir um perfeito funcionamento da rede e satisfação dos seus usuários.

Trata-se de uma iniciativa que busca a otimização dos processos administrativos e maior eficiência operacional da gestão da Infraestrutura de Segurança do Coren-RJ, observando que o projeto busca gerar condições de fornecimento de soluções numa perspectiva de serviço de maneira que as demandas sejam atendidas de maneira mais rápida e assertiva, suportando operações que impliquem em um ambiente seguro e confiável tanto para os funcionários e colaboradores do Coren-RJ quanto para os titulares (público externo).

A contratação do serviço possibilitará qualificar a administração de TI, tornando-a efetivamente comprometida com a qualidade dos serviços, com excelência de gestão e, principalmente com as áreas de negócios do Coren-RJ.

O Coren-RJ encontra-se num momento de crescimento e expansão, sua rede tem sido cada vez mais acessada, tornando-se imperativo que o ambiente tecnológico interno esteja disposto de forma estável, robusta e confiável. Os sistemas atualmente em uso não cobrem todas as camadas de rede do tráfego existente. Esta forma de utilização não protege o ambiente contra as vulnerabilidades existentes atualmente, o que fatalmente resultará em indisponibilidade do ambiente. Camadas de proteção avançada poderiam dotar o Coren-RJ de uma infraestrutura de segurança mais robusta e confiável.

A crescente dependência da tecnologia da informação em diversas áreas da organização torna imprescindível esse projeto com foco na segurança da informação, principalmente em face da expansão dos Sistemas Corporativos internalizados pelo Departamento de Tecnologia da Informação, Profissionais e a sociedade em geral.

Há no Coren-RJ um histórico de ataques e infestação de vírus que comprometeram a disponibilidade dos serviços da instituição, atendimento a sociedade em geral, atividades das subseções e um relatório realizado pela DTIC apresentou algumas vulnerabilidades no link internet e webmail do Coren-RJ que precisavam ser sanadas.



A principal vantagem da contratação de serviços estará na atividade de monitoramento permanente, apta a propiciar pronta resposta a eventuais incidentes ocorridos na operação diária. Esta infraestrutura estará ligada diretamente à gestão do ambiente tecnológico do Coren-RJ e será dotada de infraestrutura física, ferramentas integradas de inteligência e de comunicação, assim como sistemas tecnológicos complexos, capazes de prover informações necessárias à tomada de decisão, à emissão de ordens e ao acompanhamento de ações, que procuram como resultado final prover um ambiente mais confiável e estável aos usuários internos e externos.

Além de aumentar a segurança de toda a rede local do Coren-RJ, o serviço prevê solução de filtragem e proteção de intrusão, camada adicional contra-ataques de aplicação e serviços de resposta a incidente de segurança. O conjunto do projeto permitirá a implementação de políticas de segurança globais e/ou diferenciadas para os usuários, além de facilitar a administração dos incidentes de segurança.

A Segurança da Informação é um processo e a segurança de estações, servidores, usuários e das informações corporativas não basta ser composta apenas de antivírus e um firewall de bloqueio de portas. E as ameaças, que podem ser internas ou externas, vêm aumentando em quantidade e complexidade, demandando a utilização de soluções avançadas com múltiplas camadas de proteção, de forma a reduzir o risco, minimizando a probabilidade e os impactos de um eventual ataque cibernético.

O fluxo constante de complexas e evoluídas ameaças como worms, spywares, cavalos de Tróia, hackers, ladrões de identidade e diversos outros tipos de ataques ameaçam os dispositivos conectados à Internet. Os danos causados pelas pragas virtuais podem comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações, serviços e operações de rede, atingindo recursos essenciais para o bom funcionamento dos ativos da instituição, o que inclui seus bens tangíveis e intangíveis, como a reputação da instituição perante a sociedade.

Dessa forma, objetivando minimizar os riscos, o Coren-RJ necessita implantar uma solução corporativa de gerenciamento da segurança. A implantação da solução deverá permitir a identificação das tentativas de invasão aos sistemas do Coren-RJ, identificar e mitigar as vulnerabilidades existentes, protegendo a Instituição de uma grande gama de ataques internos e externos e visará aderência aos objetivos estratégicos e metas da “Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018, versão 1.0” cujas diretrizes aplicam-se a todos os órgãos e entidades que integram a APF.

Baseado nas motivações e fundamentações expostas apresenta-se ações que visam resolver os problemas enfrentados: (i) Implantação de uma solução que atue proativamente contra códigos maliciosos de qualquer natureza com atualizações constantes; (ii) Implantação de uma solução que analise, controle e que faça o balanceamento dos diferentes tipos de tráfego atualmente utilizados na Internet e que também compreenda os novos paradigmas de segurança baseado em comportamento, reputação e tráfego criptografado; (iii) Implantação de uma solução que gere os equipamentos diversificados que ingressam na rede corporativa do Coren-RJ pelos diversos meios, incluindo via sem fio, e que garanta que suas atividades sejam compatíveis com a finalidade do uso dos serviços disponibilizados pelo Coren-RJ e que não comprometa o bom desempenho da Rede e a segurança, mitigando potenciais vulnerabilidades; (iv) Implantação de uma solução que controle o tráfego da rede sem fio corporativa e a disponibilidade, integridade, confidencialidade e autenticidade dos dados trafegados; (v) Implantação de uma solução que controle e filtre os acessos a conteúdos e programas (softwares) nos diversos computadores e notebooks da instituição, garantindo que somente os programas e conteúdos destinados aos fins de pesquisa e desenvolvimento de trabalhos do Coren-RJ sejam acessados; (vi) Implantação de uma solução que proteja os sistemas hospedados na infraestrutura interna do Coren-RJ, e por vezes disponibilizados pela Internet para outras instituições públicas e/ou privadas e também para sociedade; (vii) Implantação de uma solução que permita a comunicação segura entre o Coren-RJ, suas subseções, o COFEN, assim como os funcionários e colaboradores que realizam atividades remotamente; (viii) Implantação de uma solução que monitore os diferentes serviços



disponibilizados pelo Coren-RJ e que são suportados em diversas plataformas tecnológicas de forma a possibilitar a atuação proativa do Departamento de TIC do Coren-RJ na manutenção da disponibilidade dos serviços e, (ix) Implantação de uma solução que investigue minuciosamente a rede corporativa do Coren-RJ, tanto na infraestrutura quanto nos sistemas e ferramentas de apoio, em busca de potenciais vulnerabilidades nos diversos serviços e estruturas, dentro e fora do Coren-RJ e que auxilie na extinção ou minimização dos riscos de eventuais vulnerabilidades.

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

A Implantação deste projeto será o primeiro passo para a modernização do parque tecnológico em todo âmbito do Coren-RJ (Sede e Subseções) que contará com a implementação de rede sem fio, com padrões de segurança, equipamentos mais modernos, seguindo as melhores práticas de segurança da informação e marco civil da internet.

### 3. DOTAÇÃO ORÇAMENTÁRIA

Considerando ainda a Previsão Orçamentária do Orçamento de 2017, na rubrica 6.2.2.1.2.44.90.52 dos Equipamentos e Material Permanente subitem 6.2.2.1.2.44.90.52.004 Equipamentos de Informática conforme PPA 2016 – 2018, A – Eixo Externo, Objetivo 2 que trata do Fortalecimento do Coren-RJ como órgão de representação, subitem 26, referente a Ampliação da Oferta de Serviços pela Internet e B – Eixo Interno, Objetivo 2 que trata da Manutenção e Aprimoramento da Infraestrutura do Coren-RJ, subitem 46, referente a Modernização e Atualização a Infraestrutura e Serviços de TI.

O DTIC verifica que as despesas decorrentes da Contratação correrão dos recursos próprios do Conselho Regional de Enfermagem do Rio de Janeiro, no exercício 2017 conforme PPA 2016 - 2018, sendo seu elemento de despesa a conta 6.2.2.1.2.44.90.52.004 – Equipamentos de Informática possuindo disponibilidade financeira para contratação do serviço.

### 4. QUANTIFICAÇÃO DOS PRODUTOS E SERVIÇOS – LOTES E ITENS

Lote	Item	Descrição	Quantidade Prevista	Forma de Desembolso	Valor Unitário
1	1	Firewall de Borda no modo Cluster Ativo/Passivo – TIPO A	2	Único	
	2	Firewall Interno com Gerenciamento Centralizado (Stand Alone) – TIPO B	12	Único	
	3	Ponto de Acesso de Comunicação para Redes sem Fio	15	Único	
	4	Implantação da Solução de Segurança	1	Único	
	5	Treinamento da Solução de Segurança	1	Único	



	6	Suporte da Solução de Segurança	1	Único	
2	1	Switch PoE de Comunicação 24 portas para Redes sem Fio	4	Único	
	2	Switch de Comunicação 48 portas	6	Único	
	3	Implantação dos Switches de Comunicação de Rede	1	Único	
	4	Treinamento dos Switches de Comunicação de rede	1	Único	
	5	Suporte aos Switches de Comunicação de rede	1	Único	
		Total			

## 5. FIREWALL DE BORDA MODO CLUSTER ATIVO/PASSIVO – TIPO A

5.1. A solução de segurança deverá ser implementado sobre uma infraestrutura de hardware e software de uso exclusivo do CONTRATANTE e dedicada para esta finalidade, do tipo appliance físico e access points wireless, projetados especificamente para as funcionalidades propostas, não sendo admitidas soluções baseadas em computadores de uso geral, devendo a empresa fornecer o cabeamento, adaptadores e demais conexões necessárias para a completa conectividade dos recursos empregados à infraestrutura do CONTRATANTE;

5.2. O sistema deve compreender minimamente as seguintes funcionalidades gerais: filtro de pacotes com controle de estado, filtro de conteúdo Web, VPN, balanceamento de carga, QoS e gerenciamento (administração) de redes wireless;

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

5.4. A solução deverá trabalhar em alta disponibilidade e pressupõe-se um par de appliances 2 (dois) equipamentos de funcionalidades idênticas, de forma que funcione com modelo de alta disponibilidade, tolerante a falhas, minimamente do tipo ATIVO/PASSIVO ou ASSIMÉTRICO, com licenciamento unificado, com todas as funções ativas, independente da falha de um dos elementos que compõem este par.

5.5. Não serão aceitas soluções baseadas em PC de uso geral ou soluções que contenham componentes do tipo acionadores de discos rígidos. Os dois dispositivos são ligados em paralelo, com réplicas do estado de conexões entre eles.

5.6. Para habilitação no certame a empresa deverá apresentar no mínimo 2 (dois) atestado que comprove aptidão técnica, expedido por pessoa jurídica de direito público ou privado. O documento deve comprovar que a licitante forneceu os mesmos equipamentos e soluções licitadas neste termo de referência, contemplando administração e monitoramento, com fornecimento de solução composta de pelo menos solução de firewall, detecção e prevenção de intrusão (IPS/IDS), filtro de conteúdo, mail relay, antispam, antivírus de rede e email e VPN (Virtual Private Network).

5.7. A Tabela de Comprovação Técnica deve conter, ainda, nome do documento comprobatório emitido pelo Fabricante específico para este edital.



- 5.8. A solução provida deverá suportar:
- 5.8.1. Suporte a no mínimo 3 (três) zonas de segurança: Externo, Privado e Opcional
  - 5.8.2. Suporte a IP dinâmico e estático em sua interface externa
  - 5.8.3. Deve suportar no mínimo 08 Gbps de largura de Banda do Firewall (throughput), apenas na função de Firewall
  - 5.8.4. Deve suportar no mínimo 1.4 Gbps de largura de Banda UTM (throughput), com recursos UTM habilitados (Gateway AV, IPS, App Control, Web Filter).
  - 5.8.5. Principais características: Firewall, VPN, WebFilter, Controle de acesso convidado (Captive Portal), Redundância de links de conexão de internet, Balanceamento de Carga, Conectividade e acesso remoto por VPN, IPSec e SSL VPN; Proteção contra conteúdo da web inadequado, ilegal e perigoso através da filtragem de conteúdo e URL; Trabalha na redução de latência para preservar a largura de banda e otimizar desempenho e apresentar relatórios analíticos relativos a tráfego de aplicativos, uso de largura de banda e de ameaças à segurança.
  - 5.8.6. Deve suportar no mínimo 3.800.000 conexões concorrentes (bi-direcionais), suportar conexões de no mínimo 300 usuários internos simultâneos, com todas as funções do firewall habilitadas;
  - 5.8.7. Suportar os seguintes mecanismos de criptografia: DES, 3DES, AES 128 - 192 - 256-bit;
  - 5.8.8. Suportar a implementação de políticas de segurança em camada 7 (Modelo OSI), mais conhecido como proxy de aplicação.
  - 5.8.9. Dois canais de comunicação com a Internet de no mínimo 100 Mbps cada, de operadoras distintas, de maneira simultânea, garantindo alta disponibilidade;
  - 5.8.10. Gerenciamento de solução de rede wireless integrada ao Firewall que será responsável pelas seguintes funções: gerenciamento, administração e configuração centralizada de no mínimo 20 (vinte) access points wireless, funções de segurança para acesso e tráfego de dados, gerenciamento de RF (Rádio Frequência) e Prevenção de Intrusão (Wireless IDS);
  - 5.8.11. Permitir a edição de políticas de segurança de forma gráfica e off-line (sem estar conectado diretamente ao appliance);
  - 5.8.12. Permitir a Edição de Políticas na Interface Gráfica do Windows, o interface web e CLI (Command Line Interface);
  - 5.8.13. Suporte de pelo menos dois perfis de administração: escrita e somente leitura;
  - 5.8.14. Proporcionar autenticação dos usuários em um servidor Windows Active Directory;
  - 5.8.15. Administração do dispositivo (appliance) deve ser inteiramente através de interface gráfica de gerenciamento fornecida pelo fabricante da solução ou via Web. Não serão aceitos softwares de terceiros;
  - 5.8.16. A solução deverá vir licenciada para no mínimo 4 dispositivos de Firewall;
  - 5.8.17. Suportar gerenciamento de todos os appliances oferecidos na solução, sem limite de software para tal tarefa;
  - 5.8.18. As interfaces de rede devem, cada uma, suportar tráfego de no mínimo 1 Gbps Full Duplex;
  - 5.8.19. Suportar no Mínimo 06 (seis) Interfaces 10/100/1000 BaseT. Estas interfaces devem ser configuradas com qualquer um dos três tipos de zonas de segurança exigidas no subitem 4.8.1;
  - 5.8.20. Suporte de Multi-Wan. O equipamento deve suportar pelo menos 04 (quatro) conexões externas à Internet. Estas interfaces devem operar em modo de tolerância a falha (fail-over) e balanceamento de carga (load balance). No mínimo 02 Interfaces SFP de 1 GB;



- 5.8.21. Suporte de alta disponibilidade ativo / passivo e ativo / ativo;
- 5.8.22. Deve suportar a execução no modo router (roteamento), o modo drop-in (o mesmo endereço IP em todas as interfaces), e em modo bridge transparente;
- 5.8.23. Deve permitir múltiplas sessões PPPoE por interface ;
- 5.8.24. Suporte para roteamento baseado em políticas (Policy Based Routing). Isso permite escolher porque o tráfego interface externa será enviado com base nos parâmetros fornecidos pelo administrador;
- 5.8.25. O appliance deve fornecer no mínimo controle de banda por interface, usuários, políticas, protocolo e grupo de usuários.
- 5.8.26. Recurso de backup das configurações que deverá ser efetivado de forma automática e enviado para um ambiente separado da solução;
- 5.8.27. Suportar autenticação via RADIUS server, SecureID, LDAP e Microsoft Active Directory
- 5.8.28. Deve oferecer suporte transparente para autenticação junto ao Microsoft Active Directory (Single Sign-On / SSO)
- 5.8.29. Não devem haver limites sobre o número de usuários online;
- 5.8.30. Suportar configuração de DNS Dinâmico (Dynamic DNS);
- 5.8.31. O appliance deve ter defesas contra ataques fragmentados. Para isso deve ser capaz de remontar pacotes fragmentados antes de enviá-los para a rede interna;
- 5.8.32. A solução deve ser capaz de filtrar o conteúdo dentro dos protocolos mais comuns. Como tal, eles devem ser capazes de filtrar por tipo de conteúdo MIME.
- 5.8.33. O appliance deve proteger os servidores de e-mail internos contra retransmissão aberta (open relay). Ele deve ser capaz de configurar os servidores para os domínios autorizados.
- 5.8.34. Deve permitir definição de limites para a detecção de ataques de inundação (flood) e negação de serviço (DoS) e negação de serviço distribuída (DDoS).
- 5.8.35. Deve suportar o protocolo de detecção de anomalias (Protocol Anomaly Detection - PAD) para o DNS e outros protocolos comuns.
- 5.8.36. O sincronismo entre as configurações como Regras de Firewall, Regras de NAT, Entidades, Contas administrativas, Configuração de VPN, Configurações de rede, Roteamento estático, Roteamento dinâmicas e filtros web.
- 5.8.37. Os equipamentos que compõem a solução deverão ter seu funcionamento restrito às suas funções, não podendo interferir ou causar lentidão no funcionamento da rede local do CONTRATANTE.
- 5.8.38. O software e o hardware empregados deverão corresponder a uma solução de notória eficácia já em uso no mercado nacional, devendo ser dimensionados e configurados de forma que não prejudique o desempenho da infraestrutura da rede do CONTRATANTE e seus serviços;
- 5.8.39. O serviço deve possibilitar a implementação de políticas de segurança orientadas a credenciais de usuários através de autenticação LDAP, NTLM, RADIUS e totalmente integrado com Microsoft AD 2012 e superiores, independentemente do endereço IP de origem;
- 5.8.40. Deve permitir o controle de acesso convidado (Captive Portal)
- 5.8.41. A CONTRATADA deverá fornecer à CONTRATANTE acesso de leitura às configurações da solução;



- 5.8.42. Os equipamentos deverão possuir robustez adequada ao tráfego de dados do CONTRATANTE.
- 5.8.43. A solução de firewall deve ser uma solução integrada composta de Hardware e Software de segurança da informação do tipo UTM (Unified Threat Management) que tenha a capacidade de integrar em um único dispositivo: filtro de pacotes com controle de estado, filtro de conteúdo WEB, VPN, balanceamento de carga, QoS, em um esquema de alta disponibilidade (dois equipamentos funcionando de forma que se um pare o outro assuma as funções do equipamento que parou);
- 5.8.44. Permitir a filtragem de pacotes através da análise do usuário, endereço de origem, endereço de destino e protocolo;
- 5.8.45. Obedecer à marcação prévia de QoS; e capacidade de trabalhar em camada 3 ou camada 2;
- 5.8.46. Suportar tráfego de IP Multicast;
- 5.8.47. Implementar Network Address Translation (NAT) e Port Address Translation (PAT);
- 5.8.48. Suporte NAT estático (Port Forwarding), NAT Dinâmico, NAT um-para-um (One-to-One), IPSec NAT Traversal e NAT baseado em políticas (Policy Based);
- 5.8.49. Possuir a capacidade de tomar a decisão de encaminhar ou bloquear um pacote, com base nos pacotes anteriores (stateful inspection);
- 5.8.50. Permitir monitoramento em tempo real de registros de tráfego de rede;
- 5.8.51. O equipamento deve suportar o gerenciamento via navegador em dispositivos móveis nas plataformas Apple IOS 6 e superior, Android 4.0 ou superior e Microsoft Windows Phone 8 ou superior, sem a necessidade de instalação de cliente nos dispositivos móveis e com redimensionamento de tela automático.
- 5.8.52. O equipamento deve permitir o gerenciamento via linha de comando por meio de uma porta serial ou através de SSH;
- 5.8.53. Alta disponibilidade da ferramenta de gerenciamento centralizado, baseado em tecnologia de Cluster; Deve permitir o envio de alarmes através de SNMP ou e-mail;
- 5.8.54. Possuir filtro de aplicações, de modo a permitir a identificação de padrões de dados dentro das conexões, possibilitando o tratamento automático (bloqueio, liberação ou redução/aumento de banda) de aplicações do tipo peer-to-peer, mensageria instantânea e download de arquivos;
- 5.8.55. Suportar tráfego VoIP e os padrões SIP e H.323;
- 5.8.56. Compatível com redes IPv4, IPv6 e redes híbridas, devendo estar em conformidade com as RFC-s pertinentes;
- 5.8.57. Permitir o controle de acesso por usuário, para plataformas Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10 de forma transparente (sem a necessidade do usuário digitar novamente a senha), para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado;
- 5.8.58. Permitir o controle de acesso por usuário, para todas as plataformas com browser através de autenticação via formulário para todos os serviços suportados, de forma que um determinado usuário tenha seu perfil de acesso automaticamente configurado;
- 5.8.59. Possuir perfis de acesso hierárquicos;
- 5.8.60. Prover mecanismo que permita a especificação da validade para regras de filtragem, individualmente (por regra), por dia da semana e horário; e permitir a visualização pela interface gráfica, em tempo real, de todas as conexões TCP e sessões UDP ativas através do dispositivo e a finalização de qualquer uma destas sessões ou conexões;



- 5.8.61. Permitir a geração de gráficos em tempo real, representando os serviços mais utilizados e as máquinas mais acessadas em dado momento;
- 5.8.62. Possibilitar o registro de toda a comunicação realizada através do firewall, e de todas as tentativas de abertura de sessões ou conexões que forem recusadas pelo mesmo;
- 5.8.63. Possuir mecanismo que permita capturar o tráfego de rede em tempo real (sniffer) via interface gráfica, com visualização em tempo real pela interface gráfica e com capacidade para exportação dos dados capturados para arquivo no mínimo em formato PCAP;
- 5.8.64. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;
- 5.8.65. Prover proteção contra os ataques de negação de serviço SYN Flood, Land, Tear Drop e Ping ODeath;
- 5.8.66. Possuir mecanismo que limite o número máximo de conexões simultâneas de um mesmo cliente para um determinado serviço e/ou servidor;
- 5.8.67. Detectar automaticamente e inserir regras de bloqueio temporárias para varreduras de portas efetuadas contra o dispositivo ou contra qualquer máquina protegida por esse, mesmo que realizados em períodos maiores que 1 (um) dia;
- 5.8.68. Permitir visualização dos sites acessados em tempo real;
- 5.8.69. Permitir a inserção de uma URL de redirecionamento para bloqueio por palavras-chave nas regras de perfil para HTTP, FTP e tipos de arquivos bloqueados;
- 5.8.70. Permitir a filtragem de URL-s, para os protocolos HTTP, HTTPS, FTP, por usuário, permitindo a definição de perfis de acesso diferenciados para cada usuário ou grupo;
- 5.8.71. Implementar Proxy transparente para o protocolo HTTP e HTTPS, de forma a dispensar a configuração dos browsers das máquinas clientes para a utilização das características dos dois itens acima;
- 5.8.72. Possuir funcionalidade de bloquear ou liberar a navegação web dependendo do navegador (browser) que o usuário estiver utilizado;
- 5.8.73. Implementar sistema que possibilite a reescrita de URL-s;
- 5.8.74. Implementar sistema que possibilite a concatenação (Stripping) de cabeçalho HTTP;
- 5.8.75. Implementar sistema que possibilite a adição de cabeçalho HTTP;
- 5.8.76. Possuir mecanismo de proxy SSL reverso, permitindo que VPN-s cliente-servidor sejam estabelecidas com o dispositivo, de forma transparente, e então redirecionadas para qualquer servidor interno da rede, sem o uso de cliente de criptografia específico e com autenticação opcional de usuários via certificados digitais padrão X.509;
- 5.8.77. Permite identificar o uso de técnicas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, como por exemplo, aplicações Skype, Ultrasurf e ataques mediante a porta 443;
- 5.8.78. Suporta a detecção de aplicações dinâmicas dentro de sessões de proxy HTTP;
- 5.8.79. Deve permitir o armazenamento em Cache de conteúdo trafegados pelo protocolo HTTP e HTTPS;
- 5.8.80. Possuir sistema de cache interno, armazenando requisições WEB em disco local;
- 5.8.81. Possibilitar a integração com servidores de cache WEB externos;



- 5.8.82. Possibilitar a integração com cache WEB externos hierárquicos utilizando ICP (Internet Cache Protocol);
- 5.8.83. Deve prover serviço VPN (Virtual Private Network) para pacotes IP e VPN SSL, integrado à Solução Firewall/UTM, com chaves de criptografia com tamanho igual ou superior a 128 bits, de forma a possibilitar a criação de canais seguros ou VPN-s através da Internet;
- 5.8.84. Suportar padrão IPSEC, de acordo com as RFCs 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão;
- 5.8.85. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;
- 5.8.86. Possibilitar mecanismo de criação de VPN-s entre máquinas Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux e Mac OS e o dispositivo, com chaves de criptografia simétricas com tamanho igual ou superior a 128 bits;
- 5.8.87. Funcionar como um provedor de VPN para clientes, de modo a atribuir aos clientes endereços IPs das redes internas, colocando-os, virtualmente, dentro das mesmas (0 hops);
- 5.8.88. Prover cliente VPN para as plataformas Windows 7, Windows 8, Windows 10, Linux e Mac OS, que permita uso de chaves criptográficas simétricas com 128 ou mais bits;
- 5.8.89. O cliente de tunelamento de rede IP deverá ser, para clientes Windows e Linux, executar com privilégios básicos de usuário comum. Esta funcionalidade não é exigida apenas durante a primeira instalação do cliente;
- 5.8.90. Deverá ser possível configurar o endereço/range IP a ser atribuído a placa de rede virtual do cliente de VPN, bem como sua máscara de rede, endereços dos servidores DNS, endereço dos servidores WINS, rota default e rotas para sub-redes;
- 5.8.91. No VPN cliente/firewall deverá ser possível a configuração do envio ou não de pacotes broadcast da rede onde o servidor se encontra para o cliente;
- 5.8.92. O cliente de VPN deverá possibilitar que seu funcionamento seja sincronizado ou não com o dial-up do Windows, possibilitando que ele estabeleça a VPN automática e imediatamente depois de se ter estabelecido uma conexão discada;
- 5.8.93. Suportar VPN Failover (reestabelecimento da VPN sobre um segundo enlace caso haja falha no enlace principal);
- 5.8.94. A solução de VPN deverá trabalhar no mínimo com os seguintes protocolos: IPSEC, PPTP, L2TP, SSL;
- 5.8.95. Possuir funcionalidade Dead Peer Detection (DPD), ou similar;
- 5.8.96. Prover funcionalidade de VPN SSL, com o estabelecimento do túnel VPN e autenticação via browser;
- 5.8.97. A conexão VPN SSL deverá ser totalmente transparente para o usuário final, de forma que seja realizado o download e instalação do Applets, assim que necessários;
- 5.8.98. Deve ter a capacidade para fazer o download do Software Client da VPN SSL direto do dispositivo;
- 5.8.99. Disponibilidade de Software SSL-Client para no mínimo: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux e Mac OS;
- 5.8.100. Deve suportar VPN móvel (Mobile VPN);
- 5.8.101. Deve suportar pelo menos 150 VPNs móveis usando IPsec;



- 5.8.102. Deve suportar pelo menos 150 usuários móveis usando SSL VPNs;
- 5.8.103. Suportar VPN entre escritórios remotos;
- 5.8.104. Deve suportar pelo menos 100 VPNs entre escritórios usando IPSec;
- 5.8.105. Suportar os seguintes mecanismos de criptografia e autenticação SHA-1, MD5, IKE Pre-Shared Key, 3rd Party Cert
- 5.8.106. Suporte para VPN Failover (re-estabelecimento da VPN no link adicional em caso de falha do link principal)
- 5.8.107. A taxa de banda disponível IPSEC VPN deve ser de no mínimo 4,4 Gbps
- 5.8.108. Proporcionar funcionalidade de Dead Peer Detection (DPD)
- 5.8.109. O aparelho deve ser capaz de interagir com qualquer outro produto de outra marca que siga o padrão IPSec.
- 5.8.110. Deverá permitir a integração de algoritmos de terceiros em seus sistemas criptográficos sem intervenção de terceiros, Hardware ou Software, sujeito exclusivamente as normas Brasileiras. Possuir capacidade de integração de algoritmos de estado, em hardware, em seu sistema criptográfico, sujeito exclusivamente as normas Brasileiras.
- 5.8.111. Possibilitar drag-and-drop (arrastar e soltar) para criação e alteração de regras, por meio da interface gráfica;
- 5.8.112. A interface gráfica deverá possuir mecanismo que permita a gerência remota de múltiplos dispositivos sem a necessidade de se executar várias interfaces;
- 5.8.113. A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e a realização das tarefas mais comuns na administração do dispositivo, incluindo a configuração de VPN-s, NAT, perfis de acesso e regras de filtragem;
- 5.8.114. Possuir mecanismo que permita a realização de cópias de segurança (backups) e restauração remota, através da interface gráfica, sem necessidade do reinício do sistema;
- 5.8.115. Deverá ser capaz de executar um backup por linha de comando e oferecer a opção de salvar o arquivo de backup localmente ou exportar usando o protocolo FTP;
- 5.8.116. Suportar o uso simultâneo de múltiplos links em um mesmo firewall (poderia ser appliance), de provedores distintos ou não, sendo o firewall o responsável por dividir o tráfego entre os distintos links;
- 5.8.117. Permitir o balanceamento de links com IPs dinâmicos para ADSL, ou outra tecnologia de banda larga que não utilize IP Fixo;
- 5.8.118. Implementar mecanismo de balanceamento de carga, permitindo com que vários servidores internos, sejam acessados externamente pelo mesmo endereço IP. O balanceamento de canal deverá monitorar os servidores internos e, em caso de queda de um destes, dividir o tráfego entre os demais, automaticamente;
- 5.8.119. Implementar mecanismo de persistência de sessão para o balanceamento de carga, através de diversas conexões, para quaisquer protocolos suportados pelos servidores sendo balanceados;
- 5.8.120. Permitir inspeção de pacotes à nível de aplicação;
- 5.8.121. Deve ser capaz liberar e bloquear de conexões e aplicativos através de análise DPI (Deep Packet Inspection) ou similar utilizando aplicações cadastradas para aplicações de Firewall com fornecimento das assinaturas de aplicações e possibilidade de adição das mesmas manualmente em caso de necessidade.



- 5.8.122. Deve prover solução de Filtro de Conteúdo Web (Web Filter) integrada à Solução Firewall/UTM e prover a funcionalidade de proxy com cache de conteúdo Web;
- 5.8.123. Capacidade de suportar a funcionalidade de filtragem de conteúdo no mesmo appliance via subscrição adicional
- 5.8.124. A filtragem de conteúdo deve incluir a opção de filtragem por categorias. Esta opção de filtro deve ser configurável também por grupos de usuários e com mínimo 140 categorias.
- 5.8.125. Ser dimensionado e configurado de forma a armazenar os resultados da sua execução (logs) em um banco de dados da própria solução que permita à CONTRATANTE a realização de consultas on-line;
- 5.8.126. Ser integrado à infraestrutura de rede existente, depois de fornecidas algumas configurações básicas de IP (endereço, gateway, servidor de DNS etc.), implementando as políticas de acesso Web;
- 5.8.127. A solução deve permitir exceções (whitelist) para filtragem de conteúdo;
- 5.8.128. Capacidade de identificar e bloquear no mínimo 1800 aplicações diferentes, incluindo o controle granular de função do aplicativo como login, transferência de arquivos e funcionalidades de redes sociais (chat, aplicativos, jogos...);
- 5.8.129. Possibilidade de atualização automática ou manual de assinaturas de aplicativos;
- 5.8.130. Ser dimensionado e configurado de forma a armazenar os resultados da sua execução (logs) em um banco de dados da própria solução que permita à CONTRATANTE a realização de consultas on-line;
- 5.8.131. Ser integrado à infraestrutura de rede existente, depois de fornecidas algumas configurações básicas de IP (endereço, gateway, servidor de DNS etc.), implementando as políticas de acesso Web;
- 5.8.132. Ser capaz de verificar solicitações Web (HTTP e HTTPS), permitindo ou negando acessos baseados em regras definidas pelo CONTRATANTE;
- 5.8.133. Implementar a identificação de usuários e grupos, para efeito de detalhamento de filtragem do acesso (liberações ou bloqueios), totalmente compatível com Microsoft Active Directory 2003, 2008 e 2012 e superiores, utilizando-se credenciais LDAP, RADIUS e endereço IP;
- 5.8.134. Implementar bloqueio de arquivos que consomem banda, como MP3, streaming (áudio e vídeo) e/ou arquivos que possam conter códigos maliciosos, como por exemplo .exe e .zip;
- 5.8.135. Ser capaz de verificar solicitações Web (HTTP e HTTPS), permitindo ou negando acessos baseados em regras definidas pelo CONTRATANTE, em agrupamento de endereços (URLs), em categorias e em subcategorias. As regras do proxy também serão definidas pelo CONTRATANTE;
- 5.8.136. Implementar mecanismos para categorizar novos sites da Web;
- 5.8.137. Implementar filtro de conteúdo Web com categorias de classificação de URLs e configuração de controle de acesso a estas categorias a serem consultadas no analisador de URLs;
- 5.8.138. Capaz de operar em modo man-in-the-middle para conexões do tipo HTTPS para controle de acesso e bloqueio a categorias, e também implementar bloqueio através do common-name do certificado do site;
- 5.9. Implementar funções de Antivírus:
- 5.9.1. Capacidade de suportar a funcionalidade Gateway Antivírus no mesmo appliance via subscrição adicional



- 5.9.2. Possibilidade de atualização automática ou manual de assinaturas de antivírus;
- 5.9.3. O antivírus deve suportar listas brancas (whitelist) personalizáveis para permitir o acesso à e-mails confiáveis de determinados domínios;
- 5.9.4. Bloqueio contra Spyware;
- 5.9.5. Verificar todos os arquivos compactados (. Zip. Tar,. Rar, gzip) com vários níveis de compressão;
- 5.9.6. O suporte para os protocolos: HTTP, FTP, SMTP, POP3;
- 5.9.7. Retorno baseado reputação de pontos (1-100) para permitir ignorar a verificação de URLs, melhorando o desempenho da solução;
- 5.9.8. O serviço deve ser capaz de bloquear sites de má reputação (histórico de vírus, spam ou outros tipos de malware) com base em informações recebidas de um serviço adicional proporcionado pelo appliance;
- 5.9.9. A taxa de banda disponível para Gateway de Antivirus de pelo menos 2.5 Gbps.
- 5.10. Implementar funções de Antispam:
  - 5.10.1. Capacidade de suporte Anti-spam via subscrição adicional da mesmo appliance;
  - 5.10.2. A tecnologia anti-spam baseado em Recurrent Pattern Detection (RPD - Recurrent Pattern Detection);
  - 5.10.3. O Antispam deve fornecer uma opção de quarentena;
  - 5.10.4. O Antispam deve integrar a análise de spam ao antivírus (detecção de surtos de vírus);
  - 5.10.5. O Antispam deve permitir bloqueio de spam de vários idiomas;
  - 5.10.6. Capacidade de bloquear spam baseado em imagens, além de spam baseado em texto;
- 5.11. Implementar funções de IPS
  - 5.11.1. Capacidade de adicionar funcionalidade IPS na mesma caixa via subscrição adicional;
  - 5.11.2. Possibilidade de atualização regular automática ou manual de assinaturas de IPS;
  - 5.11.3. O IPS deve fazer análise da camada de aplicação, e também definir o nível de gravidade do ataque para gerar alarmes;
  - 5.11.4. Bloqueio automático de fontes conhecidas de ataques;
  - 5.11.5. Suporte para protocolos: HTTP, FTP, SMTP, POP3;
  - 5.11.6. A taxa de banda disponível para IPS de pelo menos 04 Gbps;
- 5.12. Logs e Relatórios:
  - 5.12.1. A solução oferecida deve ser baseada em appliance físico ou virtual. Não serão aceitas soluções baseadas em plataforma de servidores;
  - 5.12.2. O serviço deve ser baseado em acesso seguro e com base de dados própria para o armazenamento dos Logs e Relatórios;
  - 5.12.3. Deve ser possível definir vários servidores Logs e Report;
  - 5.12.4. Os registros de transmissão devem ser devidamente criptografados e não requerer a criação de uma VPN somente para esse fim;
  - 5.12.5. Deve conter mais de 70 tipos de relatórios pré-definidos para facilitar a geração de informação pertinente;



- 5.12.6. Deve se capaz de gerar relatórios em formatos PDF;
- 5.12.7. Deve ser capaz de automatizar a geração e envio por e-mail de relatórios;
- 5.12.8. Deve fornecer um portal web para visualização de relatórios, com no mínimo dois perfis de acesso;
- 5.12.9. Deve ter capacidade de detalhar e filtrar informações baseado em usuários, aplicações, protocolos e destinos.

## **6. FIREWALL INTERNO COM GERENCIAMENTO CENTRALIZADO (STAND ALONE) – TIPO B**

- 6.1. A solução provida deverá suportar:
  - 6.1.1. A solução oferecida deve suportar no mínimo 3 (três) zonas de segurança: Externo, Privado e Opcional;
  - 6.1.2. O serviço deve possuir suporte a IP dinâmico e estático em sua interface externa;
  - 6.1.3. Largura de Banda do Firewall (throughput): Deve suportar no mínimo 400 Mbps de banda apenas como Firewall;
  - 6.1.4. Largura de Banda UTM (throughput): Deve suportar no mínimo 90 Mbps de banda com recursos UTM habilitados (Gateway AV, IPS, App Control, Web Filter);
  - 6.1.5. Deve suportar no mínimo 50.000 conexões concorrentes (bi-direcionais);
  - 6.1.6. Suportar a implementação de políticas de segurança em camada 7 (Modelo OSI), mais conhecido como proxy de aplicação;
  - 6.1.7. Suportar autenticação via RADIUS server, SecureID, LDAP e Microsoft Active Directory;
  - 6.1.8. Deve incluir pré-configurada em suas políticas de segurança para aplicação proxy os seguintes protocolos: HTTP, HTTPS, POP3, SMTP, FTP, DNS, SIP e H323;
  - 6.1.9. Deve oferecer suporte transparente para autenticação junto ao Microsoft Active Directory (Single Sign-On / SSO);
  - 6.1.10. Não devem haver limites sobre o número de usuários online;
  - 6.1.11. Suportar configuração de DNS Dinâmico (Dynamic DNS);
  - 6.1.12. O appliance deve ter defesas contra ataques fragmentados. Para isso deve ser capaz de remontar pacotes fragmentados antes de enviá-los para a rede interna;
  - 6.1.13. A solução deve ser capaz de filtrar o conteúdo dentro dos protocolos mais comuns. Como tal, eles devem ser capazes de filtrar por tipo de conteúdo MIME;
  - 6.1.14. O appliance deve proteger os servidores de e-mail internos contra retransmissão aberta (open relay). Ele deve ser capaz de configurar os servidores para os domínios autorizados;
  - 6.1.15. Deve permitir definição de limites para a detecção de ataques de inundação (flood) e negação de serviço (DoS) e negação de serviço distribuída (DDoS);
  - 6.1.16. Deve suportar o protocolo de detecção de anomalias (Protocol Anomaly Detection - PAD) para o DNS e outros protocolos comuns;
  - 6.1.17. Número de interfaces: Mínimo 3 (três) Interfaces 10/100/1000 BaseT. Estas interfaces devem ser configuradas com qualquer um dos três tipos de zonas de segurança exigidas 5.1.1;
  - 6.1.18. No mínimo 2 Antenas internas para conexão WIFI;



- 6.1.19. Possibilitar criação de redes WIFI seguras e Seguras;
- 6.1.20. Viabilizar integração de Rede WIFI com redes físicas por regras de Firewall;
- 6.1.21. Deve suportar um mínimo de 10 VLANs;
- 6.1.22. O appliance deve fornecer no mínimo controle de banda por interface, usuários, políticas, protocolo e grupo de usuários;
- 6.1.23. Deve suportar a execução no modo router (roteamento), o modo drop-in (o mesmo endereço IP em todas as interfaces), e em modo bridge transparente;
- 6.1.24. Suporte de alta disponibilidade ativo / passivo e ativo / ativo;
- 6.1.25. Múltiplas sessões PPPoE por interface;
- 6.1.26. Suporte para roteamento baseado em políticas (Policy Based Routing). Isso permite escolher porque o tráfego interface externa será enviado com base nos parâmetros fornecidos pelo administrador;
- 6.1.27. Suporte NAT e PAT;
- 6.1.28. Suporte NAT estático (Port Forwarding), NAT Dinâmico, NAT um-para-um (One-to-One), IPSec NAT Traversal e NAT baseado em políticas (Policy Based);
- 6.1.29. Suporte para VPN móvel (Mobile VPN);
- 6.1.30. Deve suportar pelo menos 5 VPNs móveis usando IPSec;
- 6.1.31. Deve suportar pelo menos 5 usuários móveis usando SSL VPNs;
- 6.1.32. Habilidade para fazer o download do Software cliente SSL a partir do firewall;
- 6.1.33. Disponibilidade de cliente software SSL para Windows XP, Windows Vista, Windows 7, 8 e MAC OSx;
- 6.1.34. Suportar VPN entre escritórios remotos;
- 6.1.35. Deve suportar pelo menos 5 VPNs entre escritórios usando IPSec;
- 6.1.36. O aparelho deve ser capaz de interagir com qualquer outro produto de outra marca que siga o padrão IPSec;
- 6.1.37. Suportar os seguintes mecanismos de criptografia: DES, 3DES, AES 128 - 192 - 256-bit;
- 6.1.38. Suportar os seguintes mecanismos de criptografia e autenticação SHA-1, MD5, IKE Pre-Shared Key, 3rd Party Cert;
- 6.1.39. Proporcionar funcionalidade de Dead Peer Detection (DPD);
- 6.1.40. Suporte para VPN Failover (re-estabelecimento da VPN no link adicional em caso de falha do link principal);
- 6.1.41. A taxa de banda disponível IPSEC VPN deve ser de no mínimo 4,4 Gbps;
- 6.1.42. Filtragem de Conteúdo Web e Controle de Aplicações.
- 6.1.43. Capacidade de suportar a funcionalidade de filtragem de conteúdo no mesmo appliance via subscrição adicional;
- 6.1.44. A filtragem de conteúdo deve incluir a opção de filtragem por categorias. Esta opção de filtro deve ser configurável também por grupos de usuários e com mínimo 140 categorias;
- 6.1.45. A solução deve permitir exceções (whitelist) para filtragem de conteúdo;



6.1.46. Capacidade de identificar e bloquear no mínimo 1800 aplicações diferentes, incluindo o controle granular de função do aplicativo como login, transferência de arquivos e funcionalidades de redes sociais (chat, aplicativos, jogos...);

6.1.47. Possibilidade de atualização automática ou manual de assinaturas de aplicativos;

## 6.2. Implementar funções de Antivírus

6.2.1. Capacidade de suportar a funcionalidade Gateway Antivírus no mesmo appliance via subscrição adicional;

6.2.2. Possibilidade de atualização automática ou manual de assinaturas de antivírus;

6.2.3. O antivírus deve suportar listas brancas (whitelist) personalizáveis para permitir o acesso à e-mails confiáveis de determinados domínios;

6.2.4. Bloqueio contra Spyware;

6.2.5. Verificar todos os arquivos compactados (. Zip, Tar., Rar, gzip) com vários níveis de compressão;

6.2.6. O suporte para os protocolos: HTTP, FTP, SMTP, POP3;

6.2.7. Retorno baseado reputação de pontos (1-100) para permitir ignorar a verificação de URLs, melhorando o desempenho da solução;

6.2.8. O serviço deve ser capaz de bloquear sites de má reputação (histórico de vírus, spam ou outros tipos de malware) com base em informações recebidas de um serviço adicional proporcionado pelo appliance

6.2.9. A taxa de banda disponível para Gateway de Antivírus de pelo menos 2.5 Gbps;

## 6.3. Implementar funções de Antispam

6.3.1. Capacidade de suporte Anti-spam via subscrição adicional da mesmo appliance;

6.3.2. A tecnologia anti-spam baseado em Recurrent Pattern Detection (RPD - Recurrent Pattern Detection);

6.3.3. O Antispam deve fornecer uma opção de quarentena;

6.3.4. O Antispam deve integrar a análise de spam ao antivírus (detecção de surtos de vírus);

6.3.5. O Antispam deve permitir bloqueio de spam de vários idiomas;

6.3.6. Capacidade de bloquear spam baseado em imagens, além de spam baseado em texto;

## 6.4. Implementar funções de IPS

6.4.1. Capacidade de adicionar funcionalidade IPS na mesma caixa via subscrição adicional;

6.4.2. Possibilidade de atualização regular automática ou manual de assinaturas de IPS;

6.4.3. O IPS deve fazer análise da camada de aplicação, e também definir o nível de gravidade do ataque para gerar alarmes;

6.4.4. Bloqueio automático de fontes conhecidas de ataques;

6.4.5. Suporte para protocolos: HTTP, FTP, SMTP, POP3;

6.4.6. A taxa de banda disponível para IPS de pelo menos 04 Gbps;

6.4.7. Gerenciamento



- 6.4.8. Administração do appliance deve ser inteiramente através de interface gráfica de gerenciamento fornecida pelo fabricante da solução ou via Web. Não serão aceitos softwares de terceiros;
- 6.4.9. Permitir monitoramento em tempo real de registros de tráfego de rede;
- 6.4.10. Deve permitir o envio de alarmes através de SNMP ou e-mail;
- 6.4.11. Deve permitir a criação de VPNs entre appliances via drag-and-drop;
- 6.4.12. Suportar gerenciamento de todos os appliances oferecidos na solução, sem limite de software para tal tarefa;
- 6.4.13. Permitir a edição de políticas de segurança de forma gráfica e off-line (sem estar conectado diretamente ao appliance);
- 6.4.14. Permitir a Edição de Políticas na Interface Gráfica do Windows, o interface web e CLI (Command Line Interface);
- 6.4.15. Suporte de pelo menos dois perfis de administração: escrita e somente leitura;
- 6.4.16. Proporcionar autenticação dos usuários em um servidor Windows Active Directory;
- 6.4.17. O equipamento deve suportar o gerenciamento via navegador em dispositivos móveis nas plataformas Apple IOS 6 e superior, Android 4.0 ou superior e Microsoft Windows Phone 8 ou superior, sem a necessidade de instalação de cliente nos dispositivos móveis e com redimensionamento de tela automático.
- 6.4.18. O equipamento deve permitir o gerenciamento via linha de comando por meio de uma porta serial ou através de SSH;
- 6.4.19. Alta disponibilidade da ferramenta de gerenciamento centralizado, baseado em tecnologia de Cluster;
- 6.4.20. Fornecer ferramenta de comparação de políticas, apontando as diferenças entre elas;
- 6.5. Logs e Relatórios
  - 6.5.1. A solução oferecida deve ser baseada em appliance físico ou virtual. Não serão aceitas soluções baseadas em plataforma de servidores;
  - 6.5.2. O serviço deve ser baseado em acesso seguro e com base de dados própria para o armazenamento dos Logs e Relatórios;
  - 6.5.3. Deve ser possível definir vários servidores Logs e Report;
  - 6.5.4. Os registros de transmissão devem ser devidamente criptografados e não requerer a criação de uma VPN somente para esse fim;
  - 6.5.5. Deve conter mais de 70 tipos de relatórios pré-definidos para facilitar a geração de informação pertinente;
  - 6.5.6. Deve se capaz de gerar relatórios em formatos PDF;
  - 6.5.7. Deve ser capaz de automatizar a geração e envio por e-mail de relatórios;
  - 6.5.8. Deve fornecer um portal web para visualização de relatórios, com no mínimo dois perfis de acesso;
  - 6.5.9. Deve ter capacidade de detalhar e filtrar informações baseado em usuários, aplicações, protocolos e destinos;



## 7. PONTO DE ACESSO DE COMUNICAÇÃO PARA REDES SEM FIO

7.1. O appliance UTM deve funcionar como controlador de access point wireless, capaz de administrar e configurar remotamente estes dispositivos, aplicando regras de segurança para as redes wireless e exibindo as seguintes informações:

7.1.1. Listagem de access point wireless.

7.1.2. Informações de configuração access point wireless.

7.1.3. Utilização da rede.

7.1.4. Listagem de clientes wireless.

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

7.2. Equipamento do Tipo Indoor

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

7.4. Deverá fornecer cobertura total e com qualidade no ambiente físico do CONTRATANTE utilizando para isso no mínimo 10 (dez) access point wireless;

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

7.6. Com no mínimo 2 rádios de frequência 5 e 2.4 GHz;

7.7. Deve atender as seguintes bandas de frequência: 2.400-2.474GHz, 5.150-5.250GHz, 5.250-5.350GHz, 5.470-5.725GHz, 5.725-5.850GHz;

7.8. O Equipamento de WIFI deve conter no mínimo 6 antenas internas omnidirecional;

7.9. O aparelho de WIFI deve ser gerenciado pelos firewall do Tipo A sem restrições;

7.10. Deverá operar para conexão a rede local com uma interface, com conector RJ-45 Fêmea;

7.11. Deverá permitir sua energização, pela interface de rede descrita no item anterior, através de um único injetor padrão IEEE 802.3af PoE, fornecido junto com cada access point;

7.12. Deverá possuir LEDs indicativos do estado de operação;

7.13. Deve conter no mínimo 01 Interface Gbe;

7.14. O aparelho de wifi deve suportar a carga de até 1.70Gbps

7.15. Deverá suportar alimentação de energia por POE 802.3af/at;

7.16. Deve possibilitar habilitar segurança para SSID dos seguintes modos: WPA-PSK, WPA2-PSK, WPA-PSK/WPA2-PSK (Misto) WPA-802.1X (Enterprises) WPA2-802.1X, WPA-802.1X/WPA2-802.1X (Misto) TKIP, AES, TKIP/AES, Captive Portal, MAC whitelist/blacklist, VLAN Tagging;

7.17. Não devem haver limites sobre o número de usuários online;

7.18. Deve conter as seguintes certificações Wireless: FCC, IC, CE e MIC;

7.19. Os aparelhos de WIFI devem poder trabalhar na umidade relativa de 5% a 90%;

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

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



- 7.21.1. Listagem de access point wireless;
- 7.21.2. Informações de configuração access point wireless;
- 7.21.3. Utilização da rede;
- 7.21.4. Listagem de clientes wireless;
- 7.21.5. Detalhes dos access point wireless não autorizados (rogues) detectados;
- 7.22. Caso seja fornecida a solução com access points em modo auto-gerenciado, deverá possuir as seguintes características:
- 7.23. Implementar funcionamento em modo auto-gerenciado, sem necessidade de controladora wireless para configuração de seus parâmetros de rede wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF. Deve obedecer a todas as características descritas mesmo neste modo de funcionamento;
- 7.24. Deve ser redundante dentro do cluster e não deve depender única e exclusivamente de um elemento do cluster, ou seja, em caso de falha de um ou mais pontos de acesso, a solução deve continuar funcionando, mesmo que somente com um único ponto de acesso;
- 7.25. Deve disponibilizar um firewall statefull interno à solução, com definição das políticas baseadas na identidade do usuário autenticado;
- 7.26. O ponto de acesso deve permitir a conversão de modo auto-gerenciado para modo gerenciado por controlador WLAN através de interface gráfica, em browser padrão (HTTPS), e permitir que todos os demais pontos de acesso pertencentes ao mesmo cluster, também seja convertidos automaticamente;
- 7.27. Deve disponibilizar na interface gráfica informações de usuários conectados, qualidade de sinal e tráfego de dados na rede.
- 7.28. Devem ser fornecidos access points wireless que atendam no mínimo as seguintes características:
  - 7.28.1. Deverá possuir e acompanhar componentes que permita sua fixação em teto e parede;
  - 7.28.2. Deverá atender simultaneamente aos padrões 802.11 b/g/n/ac 2.4GHz e 5GHz;
  - 7.28.3. Deverá operar para conexão a rede local com no mínimo uma interface GIGABIT Ethernet, com conector RJ-45 Fêmea;
  - 7.28.4. Deverá permitir sua energização, pela interface de rede descrita no item anterior, no padrão IEEE 802.3at PoE;
  - 7.28.5. Deverá possuir LEDs indicativos do estado de operação;
  - 7.28.6. Deverá possuir no mínimo 6 (seis) antenas internas (no mínimo 3X3 MIMO) ao access points wireless, em conformidade com o padrão IEEE 802.11a/b/g/n/ac;
  - 7.28.7. Deverá selecionar automaticamente o canal de transmissão;
  - 7.28.8. Deverá possuir suporte a pelo menos 08 (oito) SSIDs;
  - 7.28.9. Deverá permitir habilitar e desabilitar a divulgação do SSID;
  - 7.28.10. Deverá implementar Fast Roaming ou funcionalidade similar de forma a garantir o roaming sem perda de conexão e com integridade de sessão, dando suporte a aplicações em tempo real;
  - 7.28.11. Deverá ser implantado o protocolo de autenticação Radius para acesso wireless a rede corporativa;
  - 7.28.12. Deverá ter filtros de acesso à rede baseados em endereços MAC;



- 7.28.13. Deverá fornecer acesso a internet para a rede wireless visitante através de HotSpot;
- 7.28.14. Deverá suportar otimizações no portal de access point wireless (Hotspot) para atender as necessidades do CONTRATANTE;
- 7.28.15. Deverá suportar acesso wireless a celulares, tablets e outros;
- 7.28.16. Visando a redundância da solução de rede sem fio, os access points deverão fornecer acesso à rede independentemente do controlador, ou caso contrário, deverá ser ofertado um controlador redundante;
- 7.28.17. O equipamento deverá possuir registro de homologação na ANATEL;
- 7.29. Deverá implementar Fast Roaming ou funcionalidade similar de forma a garantir o roaming sem perda de conexão e com integridade de sessão, dando suporte a aplicações em tempo real;
- 7.30. Deverá ser implantado o protocolo de autenticação Radius para acesso wireless a rede corporativa;
- 7.31. Deverá ter filtros de acesso à rede baseados em endereços MAC;
- 7.32. Deverá fornecer acesso a internet para a rede wireless visitante através de HotSpot;
- 7.33. Deverá suportar otimizações no portal de access point wireless (Hotspot) para atender as necessidades do CONTRATANTE;
- 7.34. Deverá suportar acesso wireless a celulares, tablets e outros.
- 7.35. Permitir que a administração de WLAN seja feita através da interface Ethernet ou através da interface WLAN;
- 7.36. Permitir desabilitar a administração via WLAN;
- 7.37. Permitir a seleção do país de instalação do ponto de acesso;
- 7.38. Realizar atualização de sistema operacional do ponto de acesso utilizando os protocolos FTP, TFTP ou SCP;
- 7.39. Permitir conexão SSH via wireless ao ponto de acesso;
- 7.40. Permitir a criação de filtros que possibilitem a ativação ou desativação dos seguintes serviços: SSH, Telnet, Ping, SNMP;

## **8. SWITCH PoE DE COMUNICAÇÃO PARA REDES SEM FIO**

- 8.1. Permitir instalação em gabinete de 19" (dezenove polegadas) sem adaptações/kits.
- 8.2. LEDs de identificação de atividades de status do sistema, de cada porta e de alimentação.
- 8.3. Fonte de alimentação AC de 100/240 V, 60 Hz, com chaveamento automático.
- 8.4. Possuir altura de no máximo 1U.
- 8.5. Suportar operação normal em temperaturas de 5°C até 40°C.
- 8.6. Possuir 24 portas GigabitEthernet 1000Base-T autosense e autonegociável com suporte a conectores RJ-45 de acordo com o padrão IEEE 802.3ab. As portas deverão ser compatíveis com Fast Ethernet 100BASE-TX no padrão IEEE 802.3u.
- 8.7. Possuir, no mínimo, 2 (duas) portas 10GE com suporte à inserção de transceivers do tipo SFP+ (compatíveis com padrão IEEE 802.3ae).
- 8.8. Deverão ser fornecidos 2 (dois) cabos e 4 (quatro) módulos para uplink a 10 (dez) Gbps.



- 8.9. Implementar Power Over Ethernet (PoE) de acordo com o padrão IEEE 802.3at em todas as portas ethernet 10/100/1000 simultaneamente.
- 8.10. Arquitetura de switch Stackable (pilha), permitindo o empilhamento de no mínimo 6 (seis) unidades por caminhos redundantes através de cabo do tipo closed-loop, e com desempenho mínimo de 10 (dez) Gbps full-duplex por porta de empilhamento, não podendo ser utilizados portas Ethernet e as portas de uplink para empilhamento.
- 8.11. Deverão ser fornecidos 1 (hum) cabo e 2 (dois) módulos para o empilhamento a 10 (dez) Gbps.
- 8.12. Deve ser possível adicionar novos switches na pilha através de forma automática, sem configuração prévia do novo switch adicionado.
- 8.13. A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha além de permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.
- 8.14. Possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface DB9 ou USB ou RJ-45.
- 8.15. Deverá ser fornecido cabo de console compatível com a porta de console do equipamento a partir de computador equipado com porta USB, bem como o cabo para permitir o empilhamento.
- 8.16. Capacidade de comutação de no mínimo 88 (oitenta e oito) Gbps non-blocking, ou seja, 44 (quarenta e quatro) Gbps entrando e saindo simultaneamente.
- 8.17. Capacidade de encaminhamento de pacotes de no mínimo 33 (trinta e três) Mpps non-blocking com pacotes de, no máximo 128 (cento e vinte e oito) bytes, incluso cabeçalhos ethernet, TCP/UDP e Ipv4/IPv6.
- 8.18. Capacidade de armazenamento de no mínimo 8.000 (oito mil) endereços MAC.
- 8.19. Implementar a configuração de no mínimo 4000 (quatro mil) Vlans Ids.
- 8.20. Implementar a configuração de no mínimo 255 (duzentos e cinquenta e cinco) VLANs ativas simultaneamente.
- 8.21. Implementar as seguintes funcionalidades/padrões:
- 8.22. Padrão IEEE 802.3x (Flow Control);
- 8.23. Padrão IEEE 802.1d (Spanning Tree);
- 8.24. Padrão IEEE 802.1w (Rapid Spanning Tree);
- 8.25. Padrão IEEE 802.1s (Multiple Spanning Tree);
- 8.26. Padrão IEEE 802.3ad (Link Aggregation);
- 8.27. Padrão IEEE 802.1p (CoS – Class of Service);
- 8.28. Padrão IEEE 802.1x (Network Access Control);
- 8.29. VLANs segundo o padrão IEEE 802.1q;
- 8.30. IGMPv1, IGMPv2 e IGMPv3 snooping;
- 8.31. DHCP snooping ou funcionalidade similar que permita o bloqueio de servidores DHCP não autorizados na rede;



- 8.32. Espelhamento do tráfego de entrada e saída de múltiplas portas do switch em uma única porta, inclusive entre portas de diferentes unidades de uma pilha;
- 8.33. Espelhamento do tráfego de entrada e saída de múltiplas VLANs do switch em uma única porta, inclusive entre portas de diferentes unidades de uma pilha;
- 8.34. Mecanismos que viabilizem a limitação e controle do broadcast;
- 8.35. Mecanismos de proteção contra Destination Lookup Failure;
- 8.36. Mecanismos de proteção contra arp spoofing;
- 8.37. Encaminhamento de Jumbo Frames com tamanho mínimo de 9000 bytes nas portas Gigabit Ethernet;
- 8.38. Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED;
- 8.39. Implementar reconhecimento de Telefones IP e provisioná-los na VLAN de voz automaticamente.
- 8.40. Implementar IPv6.
- 8.41. Implementar a configuração de endereços IPv6 para gerenciamento.
- 8.42. Implementar resolução de endereços IPv4 e IPv6 (via consultas DNS) para nomes (hostnames) atribuídos aos ativos de rede.
- 8.43. Implementar ICMPv6 com as seguintes funcionalidades: ICMP request, ICMP Reply e ICMP Neighbor Discovery Protocol (NDP).
- 8.44. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet e SNMP sobre Ipv6.
- 8.45. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
- 8.46. Implementar roteamento estático para os protocolos IPv4 e Ipv6.
- 8.47. Implementar limitação de tráfego de entrada permitindo variar a taxa de limitação com granularidade de 1 (um) Mbps por porta.
- 8.48. Implementar pelo menos 8 (oito) filas de QoS em Hardware por porta 1GE .
- 8.49. Implementar funcionalidades de controle e limitação de tráfego por classe de serviço.
- 8.50. Implementar classificação e marcação de pacotes baseada em endereço de origem.
- 8.51. Implementar classificação e marcação de pacotes baseada em porta de origem.
- 8.52. Implementar classificação e marcação de pacotes baseada em endereço de destino.
- 8.53. Implementar classificação e marcação de pacotes baseada em porta de destino.
- 8.54. Implementar classificação e marcação de pacotes baseada em marcação DSCP.
- 8.55. Implementar classificação e marcação de pacotes baseada em marcação IP Precedence.
- 8.56. Implementar classificação e marcação de pacotes baseada em CoS (“Class of Service” – nível 2).
- 8.57. Implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- 8.58. Implementar controle de acesso por porta segundo o padrão IEEE 802.1x, com configuração dinâmica da VLAN do usuário autenticado.



- 8.59. Ao considerar o padrão 802.1x, implementar configuração automática de VLAN de quarentena para a porta de dispositivos/usuários não autenticados.”.
- 8.60. Caso o dispositivo a ser conectado não possua cliente IEEE 802.1x, o switch o posicionará em uma VLAN default.
- 8.61. Implementar autenticação ao menos 2 (dois) dispositivos 802.1x por porta, para suporte à autenticação de sistemas operacionais virtualizados.
- 8.62. Implementar autenticação de dispositivos baseado no endereço MAC, via servidor RADIUS ou TACACS.
- 8.63. Implementar limitação de endereços MAC por porta. Os endereços MAC podem ser aprendidos automaticamente ou configurados manualmente.
- 8.64. Implementar listas de controle de acesso (ACLs), ou funcionalidade similar, baseadas em endereços MAC de origem e destino, endereços IP de origem e destino, portas TCP e UDP.
- 8.65. Implementar definição de grupos de usuários, com diferentes níveis de acesso, ou possuir no mínimo 3 grupos de usuários pré-configurado.
- 8.66. Implementar controle de comandos para usuários ou grupos de usuários no equipamento
- 8.67. Implementar e suportar TACACS+ ou similar. O similar deve funcionar minimamente sobre TCP e ainda tratar os processos de Autenticação e autorização em separado.
- 8.68. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- 8.69. Implementar Private VLAN ou funcionalidade similar que permita segmentar uma VLAN em sub-domínios: uma VLAN primária e múltiplas VLANs secundárias.
- 8.70. Implementar gerenciamento da pilha de switches através de um único endereço IP.
- 8.71. Implementar os seguintes protocolos e funcionalidades de gerenciamento:
- 8.72. Secure Shell (SSHv2);
- 8.73. SNMPv2c e SNMPv3, com autenticação e criptografia;
- 8.74. CLI (Command Line Interface);
- 8.75. Syslog;
- 8.76. Gerenciamento por meio de interface gráfica (web browser) pelo protocolo HTTPS;
- 8.77. FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol) ou SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol);
- 8.78. NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 8.79. Implementar capacidade de monitoração via comando de operação SNMP de, no mínimo:
- 8.80. de tráfego de interfaces;
- 8.81. de uso de CPU do processador;
- 8.82. de uso de memória do processador;
- 8.83. Implementar a MIB II - RFC 1213.
- 8.84. Implementar múltiplas imagens de firmware ou permitir a atualização da imagem por intermédio de download de servidor de rede.



- 8.85. Implementar versão do sistema operacional/firmware mais recente, ou seja, o equipamento deverá possuir a versão mais atual do sistema operacional na data da autorização do fornecimento.
- 8.86. Implementar o download e o upload de configurações.

## **9. SWITCH DE COMUNICAÇÃO PARA REDES**

- 9.1. Permitir instalação em gabinete de 19" (dezenove polegadas) sem adaptações/kits.
- 9.2. LEDs de identificação de atividades de status do sistema, de cada porta e de alimentação.
- 9.3. Fonte de alimentação AC de 100/240 V, 60 Hz, com chaveamento automático.
- 9.4. Possuir altura de no máximo 1U.
- 9.5. Suportar operação normal em temperaturas de 5°C até 40°C.
- 9.6. Possuir 48 portas GigabitEthernet 1000Base-T autosense e autonegociável com suporte a conectores RJ-45 de acordo com o padrão IEEE 802.3ab. As portas deverão ser compatíveis com Fast Ethernet 100BASE-TX no padrão IEEE 802.3u.
- 9.7. Possuir, no mínimo, 2 (duas) portas 10GE com suporte à inserção de transceivers do tipo SFP+ (compatíveis com padrão IEEE 802.3ae).
- 9.8. Arquitetura de switch Stackable (pilha), permitindo o empilhamento de no mínimo 6 (seis) unidades por caminhos redundantes através de cabo do tipo closed-loop, e com desempenho mínimo de 10 (dez) Gbps full-duplex por porta de empilhamento, não podendo ser utilizados portas Ethernet e as portas de uplink para empilhamento.
- 9.9. Deverão ser fornecidos 1 (hum) cabo e 2 (dois) módulos para o empilhamento a 10 (dez) Gbps.
- 9.10. Deve ser possível adicionar novos switches na pilha através de forma automática, sem configuração prévia do novo switch adicionado.
- 9.11. A pilha deverá ser gerenciada através de um único endereço IP, permitir agregação lógica de links utilizando qualquer porta da pilha além de permitir espelhamento de portas de qualquer porta para qualquer porta da pilha.
- 9.12. Possuir porta de console para ligação direta e através de terminal RS-232 para acesso à interface de linha de comando. Poderá ser fornecida porta de console com interface DB9 ou USB ou RJ-45.
- 9.13. Deverá ser fornecido cabo de console compatível com a porta de console do equipamento a partir de computador equipado com porta USB, bem como o cabo para permitir o empilhamento.
- 9.14. Capacidade de comutação de no mínimo 88 (oitenta e oito) Gbps non-blocking, ou seja, 44 (quarenta e quatro) Gbps entrando e saindo simultaneamente.
- 9.15. Capacidade de encaminhamento de pacotes de no mínimo 33 (trinta e três) Mpps non-blocking com pacotes de, no máximo 128 (cento e vinte e oito) bytes, incluso cabeçalhos ethernet, TCP/UDP e Ipv4/Ipv6.
- 9.16. Capacidade de armazenamento de no mínimo 8.000 (oito mil) endereços MAC.
- 9.17. Implementar a configuração de no mínimo 4000 (quatro mil) Vlans Ids.
- 9.18. Implementar a configuração de no mínimo 255 (duzentos e cinquenta e cinco) VLANs ativas simultaneamente.
- 9.19. Implementar as seguintes funcionalidades/padrões:



- 9.20. Padrão IEEE 802.3x (Flow Control);
- 9.21. Padrão IEEE 802.1d (Spanning Tree);
- 9.22. Padrão IEEE 802.1w (Rapid Spanning Tree);
- 9.23. Padrão IEEE 802.1s (Multiple Spanning Tree);
- 9.24. Padrão IEEE 802.3ad (Link Aggregation);
- 9.25. Padrão IEEE 802.1p (CoS – Class of Service);
- 9.26. Padrão IEEE 802.1x (Network Access Control);
- 9.27. VLANs segundo o padrão IEEE 802.1q;
- 9.28. IGMPv1,IGMPv2 e IGMPv3 snooping;
- 9.29. DHCP snooping ou funcionalidade similar que permita o bloqueio de servidores DHCP não autorizados na rede;
- 9.30. Espelhamento do tráfego de entrada e saída de múltiplas portas do switch em uma única porta, inclusive entre portas de diferentes unidades de uma pilha;
- 9.31. Espelhamento do tráfego de entrada e saída de múltiplas VLANs do switch em uma única porta, inclusive entre portas de diferentes unidades de uma pilha;
- 9.32. Mecanismos que viabilizem a limitação e controle do broadcast;
- 9.33. Mecanismos de proteção contra Destination Lookup Failure;
- 9.34. Mecanismos de proteção contra arp spoofing;
- 9.35. Encaminhamento de Jumbo Frames com tamanho mínimo de 9000 bytes nas portas Gigabit Ethernet;
- 9.36. Implementar os protocolos LLDP (IEEE 802.1ab) e LLDP-MED;
- 9.37. Implementar reconhecimento de Telefones IP e provisioná-los na VLAN de voz automaticamente.
- 9.38. Implementar IPv6.
- 9.39. Implementar a configuração de endereços IPv6 para gerenciamento.
- 9.40. Implementar resolução de endereços IPv4 e IPv6 (via consultas DNS) para nomes (hostnames) atribuídos aos ativos de rede.
- 9.41. Implementar ICMPv6 com as seguintes funcionalidades: ICMP request, ICMP Reply e ICMP Neighbor Discovery Protocol (NDP).
- 9.42. Implementar protocolos de gerenciamento Ping, Traceroute, Telnet e SNMP sobre Ipv6.
- 9.43. Implementar mecanismo de Dual Stack (IPv4 e IPv6), para permitir migração de IPv4 para IPv6.
- 9.44. Implementar roteamento estático para os protocolos IPv4 e Ipv6.
- 9.45. Implementar limitação de tráfego de entrada permitindo variar a taxa de limitação com granularidade de 1 (um) Mbps por porta.
- 9.46. Implementar pelo menos 8 (oito) filas de QoS em Hardware por porta 1GE .
- 9.47. Implementar funcionalidades de controle e limitação de tráfego por classe de serviço.
- 9.48. Implementar classificação e marcação de pacotes baseada em endereço de origem.



- 9.49. Implementar classificação e marcação de pacotes baseada em porta de origem.
- 9.50. Implementar classificação e marcação de pacotes baseada em endereço de destino.
- 9.51. Implementar classificação e marcação de pacotes baseada em porta de destino.
- 9.52. Implementar classificação e marcação de pacotes baseada em marcação DSCP.
- 9.53. Implementar classificação e marcação de pacotes baseada em marcação IP Precedence.
- 9.54. Implementar classificação e marcação de pacotes baseada em CoS (“Class of Service” – nível 2).
- 9.55. Implementar os seguintes algoritmos de fila: Strict Priority e Round Robin com distribuição de pesos WRR (Weighted Round Robin) ou SRR (Shaped Round Robin).
- 9.56. Implementar controle de acesso por porta segundo o padrão IEEE 802.1x, com configuração dinâmica da VLAN do usuário autenticado.
- 9.57. Ao considerar o padrão 802.1x, implementar configuração automática de VLAN de quarentena para a porta de dispositivos/usuários não autenticados.”.
- 9.58. Caso o dispositivo a ser conectado não possua cliente IEEE 802.1x, o switch o posicionará em uma VLAN default.
- 9.59. Implementar autenticação ao menos 2 (dois) dispositivos 802.1x por porta, para suporte à autenticação de sistemas operacionais virtualizados.
- 9.60. Implementar autenticação de dispositivos baseado no endereço MAC, via servidor RADIUS ou TACACS.
- 9.61. Implementar limitação de endereços MAC por porta. Os endereços MAC podem ser aprendidos automaticamente ou configurados manualmente.
- 9.62. Implementar listas de controle de acesso (ACLs), ou funcionalidade similar, baseadas em endereços MAC de origem e destino, endereçosIP de origem e destino, portas TCP e UDP.
- 9.63. Implementar definição de grupos de usuários, com diferentes níveis de acesso, ou possuir no mínimo 3 grupos de usuários pré-configurado.
- 9.64. Implementar controle de comandos para usuários ou grupos de usuários no equipamento
- 9.65. Implementar e suportar TACACS+ ou similar. O similar deve funcionar minimamente sobre TCP e ainda tratar os processos de Autenticação e autorização em separado.
- 9.66. Implementar mecanismos de AAA (Authentication, Authorization e Accounting) com garantia de entrega.
- 9.67. Implementar Private VLAN ou funcionalidade similar que permita segmentar uma VLAN em sub-domínios: uma VLAN primária e múltiplas VLANs secundárias.
- 9.68. Implementar gerenciamento da pilha de switches através de um único endereço IP.
- 9.69. Implementar os seguintes protocolos e funcionalidades de gerenciamento:
- 9.70. Secure Shell (SSHv2);
- 9.71. SNMPv2c e SNMPv3, com autenticação e criptografia;
- 9.72. CLI (Command Line Interface);
- 9.73. Syslog;
- 9.74. Gerenciamento por meio de interface gráfica (web browser) pelo protocolo HTTPS;



- 9.75. FTP (File Transfer Protocol) ou TFTP (Trivial File Transfer Protocol) ou SFTP (Secure File Transfer Protocol) ou SCP (Secure Copy Protocol);
- 9.76. NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol);
- 9.77. Implementar capacidade de monitoração via comando de operação SNMP de, no mínimo:
  - 9.78. de tráfego de interfaces;
  - 9.79. de uso de CPU do processador;
  - 9.80. de uso de memória do processador;
- 9.81. Implementar a MIB II - RFC 1213.
- 9.82. Implementar múltiplas imagens de firmware ou permitir a atualização da imagem por intermédio de download de servidor de rede.
- 9.83. Implementar versão do sistema operacional/firmware mais recente, ou seja, o equipamento deverá possuir a versão mais atual do sistema operacional na data da autorização do fornecimento.
- 9.84. Implementar o download e o upload de configurações.

## **10. DETALHAMENTO DOS ITENS DO OBJETO**

### **10.1. IMPLANTAÇÃO DA SOLUÇÃO**

- 10.1.1. Os serviços de instalação física dos equipamentos devem incluir:
  - 10.1.1.1. Instalação dos Switches nos racks dos 3º, 4º, 5º e 6º andares da Sede do RJ;
  - 10.1.1.2. Instalação física dos Pontos de Acesso sem fio nos 3º, 4º, 5º e 6º andares da Sede do RJ;
  - 10.1.1.3. Instalação física e configuração lógica dos Firewalls do TIPO A no datacenter da Sede do RJ, localizada no 4º andar;
  - 10.1.1.4. Configuração lógica dos Firewalls do TIPO B, já a instalação física destes equipamentos nas Subseções será de responsabilidade da CONTRATANTE;
  - 10.1.1.5. Os serviços de instalação lógica deve incluir a configuração de todos os equipamentos (Switches, Firewalls e Ponto de Acesso sem Fio) que compõem a solução.
- 10.1.2. Os serviços de instalação lógica os Switches devem incluir:
  - 10.1.2.1. Configuração dos IPs dos switches;
  - 10.1.2.2. Configuração da conexão entre os switches;
  - 10.1.2.3. Criação de VLANs conforme necessário;
- 10.1.3. Os serviços de instalação lógica dos Firewalls devem incluir:
  - 10.1.3.1. Configuração dos IPs na Interfaces dos Firewalls;
  - 10.1.3.2. Configuração de conexão entre os Firewalls;
  - 10.1.3.3. Criação de Regras de Acesso;
  - 10.1.3.4. Criação de Filtro de Conteúdo de acordo com as necessidades do Coren-RJ;
  - 10.1.3.5. Configuração de VPN Site to Site das 10 Subseções com Sede do Coren-RJ;
  - 10.1.3.6. Configuração de acesso à interface de configuração dos Firewalls, incluindo todas as configurações que permitam a funcionalidade efetiva das funções do Firewall.



- 10.1.4 Os serviços de instalação lógica dos pontos de acesso sem fio devem incluir:
  - 10.1.4.1 Realizar um levantamento de canais disponíveis na frequência 2.4GHz e 5.8GHz a fim de escolher a frequência/canal com menos interferência de ruído;
  - 10.1.4.2 Configuração dos IPs nos Pontos de Acesso sem Fio;
  - 10.1.4.3 Configuração da conexão entre os Pontos de Acesso sem Fio e o Firewalls;
  - 10.1.4.4 Configuração das SSDIs;
  - 10.1.4.5 Configuração de SSIDs Corporativa e Visitantes com regras de acesso diferenciadas;

## **10.2. TREINAMENTO DA SOLUÇÃO**

10.2.1. A CONTRATADA deverá transferir o conhecimento da Solução de Completa (Firewalls do Tipo A e B, Pontos de Acesso sem Fio e Switches) de Redes e Segurança ofertada para uma equipe de técnicos do CONTRATANTE compreendendo as tecnologias envolvidas nos serviços contratados, assim como capacitação nos produtos e softwares utilizados para atender aos requisitos das especificações técnicas;

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

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

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

10.2.2.3 O treinamento deverá contemplar atividades práticas. Para a consecução da parte prática, poderão ser utilizados equipamentos;

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

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

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

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

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

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



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

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

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

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

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

10.2.13.1 Solução de Firewalls: mínimo de 30h/a;

10.2.13.2 Rede sem fio: mínimo de 12h/a;

10.2.13.3 Switch PoE de 24 portas: mínimo de 4h/a;

10.2.13.4 Switch de 48 Portas: mínimo de 4h/a;

10.2.14. A CONTRATADA deverá ministrar treinamento modalidade teórico e “hands on” aos técnicos do CONTRATANTE para até 5 (cinco) participantes, e deverá ser previsto duas turmas de treinamento para fins de distribuição da equipe do CONTRATANTE, sendo uma turma no período matutino e outra no período vespertino com duração de quatro (4) horas/aula por turma, por dia;

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

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

10.2.17. O treinamento será realizado na sede da CONTRATANTE;

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

### **10.3. SUPORTE TÉCNICO DA SOLUÇÃO**

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

10.3.2. O Suporte Técnico deverá cobrir a localidade do Rio de Janeiro/RJ;

10.3.3. Os serviços de suporte para os produtos devem ser disponibilizados durante 24h x 7d para todos os componentes do serviço fornecido;

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

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

10.3.6. A assistência técnica corretiva é a série de procedimentos executados para recolocar os produtos em seu perfeito estado de uso, funcionamento e desempenho, inclusive com a substituição de



componentes, partes, ajustes, reparos e demais serviços necessários de acordo com os manuais de manutenção do fabricante e normas técnicas específicas para cada caso;

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

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

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

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

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

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

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

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

10.3.15. Durante o período de garantia, a CONTRATADA compromete-se a substituir, em até 10 (dez) dias úteis, sem qualquer ônus para o CONTRATANTE, os equipamentos que apresentarem, em um período de 30 (trinta dias), duas ocorrências de defeitos por inoperância de produto ou 3 (três) ocorrências de deficiência operacional do produto, de acordo com o item 9.2.5. Neste caso, as novas unidades empregadas na substituição das defeituosas ou danificadas deverão ter prazo de garantia igual ou superior ao das substituídas;

10.3.16. A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço de atendimento com discagem gratuita (0800 ou de custo local DDD 21) ou qualquer outro meio de comunicação de disponibilidade imediata (por exemplo, sítio Web com HTTPS ou call center), sem ônus adicional para o CONTRATANTE, para chamada do serviço de suporte técnico que deverá estar acessível durante 24h x 7; horário local de Brasília.

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

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



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

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

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

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

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

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

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

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

10.3.27. Caberá à CONTRATADA monitorar de forma proativa toda a solução CONTRATADA, durante vinte e quatro (24) horas por dia, sete (7) dias por semana, garantindo os níveis de serviço acordados. Quando da detecção de problemas ou inconformidades, a CONTRATADA deverá imediatamente abrir um chamado técnico, informar à CONTRATANTE e providenciar a sua reparação dentro dos prazos estabelecidos nos acordos de níveis de serviço;

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

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

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

10.3.30.1 Patches, firmwares, fixes, correções, updates e service packs;

10.3.30.2 Novas releases, builds e funcionalidades;

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

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

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



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

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

10.3.32. A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução que deverão permanecer ativas e válidas por 24 (vinte e quatro) meses após o encerramento do Contrato sem ônus adicional para o CONTRATANTE;

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

#### **10.4. ATUALIZAÇÕES E ASSINATURAS**

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

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

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

10.4.4. A CONTRATADA deverá garantir o funcionamento adequado dos produtos durante todo o período de vigência do Contrato 36 (trinta e seis) meses e possibilitar a garantia estendida de mais 24 (vinte e quatro) meses totalizando um máximo de 60 (sessenta) meses;

10.4.5. A CONTRATADA deverá garantir a subscrição das assinaturas de definições e das bases de dados de todos os produtos e módulos integrantes da solução que deverão permanecer ativas e válidas durante todo o período de vigência do Contrato 36 (trinta e seis) meses;

10.4.6. Após encerramento do Contrato a CONTRATADA deverá garantir a subscrição das assinaturas estendidas por mais 24 (vinte e quatro) meses totalizando um máximo de 60 (sessenta) meses sem ônus adicional para o CONTRATANTE.

#### **10.5. ACORDO DE NÍVEL DE SERVIÇO (ANS) E DISPONIBILIDADE**

10.5.1. Para todas as soluções:

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

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



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

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

10.5.2. Para o Serviço de Suporte Técnico:

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

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

- Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade na solução ou em qualquer serviço que a compõe; para a criação/configuração de políticas nos firewalls; para aplicação de ações de respostas a ataque. Prazo para início do atendimento: 2 horas
- Severidade MÉDIA: Esse nível de severidade é aplicado para solicitações de criação/configuração de políticas nos demais serviços que compõem a solução; quando há problema, simultâneo ou não, nos elementos que compõem os serviços/solução, embora ainda estejam disponíveis. Prazo para início do atendimento: 4 horas
- Severidade BAIXA: Esse nível de severidade é aplicado para solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamentos. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados. Prazo para início do atendimento: 10 horas

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

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

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

- Ocorrência de 3 (três) ou mais chamados técnicos de manutenção corretiva dentro de um período contínuo de 30 (trinta) dias;
- Soma dos tempos de paralisação que ultrapasse 20 (vinte) horas dentro de um período contínuo de 30 (trinta) dias.
- No caso de inviabilidade da solução definitiva do problema apresentado no equipamento, peça e componente, independentemente do enquadramento nos casos previstos no subitem anterior, faculta-se à CONTRATADA promover a sua substituição em caráter definitivo;
- A substituição definitiva será admitida com anuência do CONTRATANTE, após prévia avaliação técnica quanto às condições de uso e compatibilidade do equipamento, peça e componente ofertado, em relação àquele que está sendo substituído;



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

10.5.2.7. O serviço contratado será considerado indisponível a partir do momento em que eventuais problemas de indisponibilidade forem registrados pelo monitoramento;

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

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

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

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

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

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

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

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

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



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

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

## **10.6. IMPLANTAÇÃO E HOMOLOGAÇÃO**

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

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

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

10.6.2.2. Políticas de configuração dos elementos da solução;

10.6.2.3. Topologia lógica para a solução;

10.6.2.4. Ações de rollback.

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

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

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

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

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

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

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

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

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

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

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



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

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

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

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

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

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

10.6.20. A CONTRATADA deverá instalar toda a solução na Sede do CONTRATANTE em até 30 (trinta) dias corridos após a assinatura do contrato. Na reunião de Alinhamento de Expectativas, deverá ser apresentado pela CONTRATADA o Plano de Implantação para análise e aprovação da CONTRATANTE;

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

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

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

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

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

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

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

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

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

10.6.29. Após o PFE, terá de ser apresentado um baseline de funcionamento normal, baseado nas recomendações do fabricante, para cada hardware/software que compõe a solução. Além disso, terão de ser apresentados relatórios periódicos contendo informações de desempenho, referentes a esses



elementos, para que seja identificada com antecedência a necessidade de adição/substituição de hardware/software. Esses relatórios serão apresentados pela CONTRATADA;

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

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

10.6.32. A solução e o suporte técnico deverão estar em plena operação e disponíveis à CONTRATANTE no prazo de, no máximo, 30 (trinta) dias corridos e contados a partir da assinatura do Contrato;

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

## **10.7. REUNIÃO PARA ALINHAMENTO DAS EXPECTATIVAS**

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

10.7.2. Deverão participar dessa reunião, no mínimo, os fiscais do Contrato, membro(s) da equipe técnica do CONTRATANTE, Interlocutor e membro(s) da equipe técnica da CONTRATADA;

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

## **10.8. RECEBIMENTO DOS SERVIÇOS**

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

## **10.9. MONITORAMENTO DO SERVIÇO**

10.9.1. As ferramentas fornecidas devem prover informações de monitoramento;

10.9.2. Esse monitoramento deve permitir, no mínimo:

10.9.2.1. Visualizar o desempenho dos equipamentos que compõem a solução, como utilização de disco, memória, CPU, tráfego na interface de rede;

10.9.2.2. Visualizar os logs dos equipamentos que compõem a solução;

10.9.2.3. Visualizar o monitoramento por meio de interface Web;

10.9.2.4. Visualizar a disponibilidade e desempenho dos elementos/serviços da solução em tempo real;

10.9.2.5. Gerar relatórios administrativos e técnicos, ambos customizáveis, em forma de textos e gráficos, com possibilidade de exportar para HTML e PDF.

10.9.3. O CONTRATANTE também realizará o monitoramento dos serviços/elementos que compõem a solução;

10.9.4. O monitoramento será utilizado para gerar relatórios mensais de disponibilidade e desempenho da solução e aplicações de penalidades.



## **11. LOCAL DE EXECUÇÃO DOS SERVIÇOS**

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

11.1.2. Os serviços serão executados nas instalações cedidas no território do CONTRATANTE, presencialmente no COREN/RJ, localizado à Avenida Presidente Vargas, nº 502, 3º, 4º, 5º e 6º Andares, Centro, Rio de Janeiro-RJ ou através de acesso remoto.

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

11.1.3.1. O serviço de configuração dos Firewalls internos do TIPO B nas Subseções do Coren-RJ será de responsabilidade da CONTRATADA.

11.1.3.2. O serviço de instalação dos Firewalls internos do TIPO B nas Subseções do Coren-RJ será de responsabilidade da CONTRATANTE, com o devido suporte remoto da CONTRATADA.

## **12. SIGILO E INVIOLABILIDADE**

12.1. A CONTRATADA compromete-se a manter em caráter confidencial as informações abaixo mencionadas, mesmo após a eventual rescisão do contrato:

12.1.1. Política de segurança adotada pelo CONTRATANTE e configurações de hardware e software decorrentes;

12.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos e atendimento aos itens de segurança, constantes do Edital de licitação;

12.1.3. Processo de implantação no ambiente do CONTRATANTE, de mecanismos de criptografia e autenticação utilizados;

12.1.4. Recomendações e implementações decorrentes do processo de consultoria;

12.1.5. Quaisquer dados que a CONTRATADA venha a ter conhecimento em decorrência da presente contratação, pertinentes a hardware, serviços e sistemas aplicativos do CONTRATANTE, cujo conhecimento por terceiros exponha o ambiente a riscos de invasão ou resulte na vulnerabilidade do mesmo.

12.1.6. Não fazer uso das informações prestadas pela CONTRATANTE que não seja em absoluto cumprimento ao contrato em questão.

12.1.7. A quebra da confidencialidade ou sigilo de informações obtidas na prestação de serviços ensejará multa, responsabilidade criminal na forma da lei, sem prejuízo de outras providências nas demais esferas.

12.1.8. A CONTRATADA obriga-se a tomar as providências necessárias para assegurar que as informações confidenciais não sejam divulgadas por seus empregados ou agentes.

## **13. COMPROVAÇÃO DAS CARACTERÍSTICAS TÉCNICAS**

13.1. O não atendimento às especificações técnicas descritas neste Termo de Referência implicará a desclassificação da proposta apresentada.

13.2. A comprovação do atendimento às características técnicas especificadas neste Termo de Referência dar-se-á por meio de catálogos, manuais e publicações originais e/ou apresentação de amostras.



13.3. A indicação do endereço eletrônico do catálogo do fabricante será aceita, como alternativa, para fins de averiguação das especificações dos produtos.

13.4. No conjunto de documentos apresentados pela licitante (folders/catálogos), para fins de aceitação, deverá vir indicando corretamente, a página, o documento e o trecho que comprove o atendimento de cada item/subitem da especificação técnica, conforme tabela abaixo.

Item/Especificação	Documento	Página	Comprovação

*Tabela de comprovação dos itens técnicos*

13.5. A proposta deverá apresentar com clareza a marca, o modelo, o tipo, a configuração e outras informações aplicáveis e necessárias à perfeita caracterização do dispositivo ou componente proposto, de forma a permitir a correta identificação deste na documentação técnica apresentada.

13.6. A proposta e a documentação técnica serão numeradas em ordem sequencial a partir da primeira página da proposta, devendo constar nesta o total de páginas.

13.7. As propostas serão analisadas por equipe de técnicos da CONTRATANTE no transcorrer do Pregão, para fins de verificação do atendimento às características da solução especificados neste Edital.

13.8. A análise técnica consistirá na verificação, por meio da documentação fornecida pela licitante ou obtida da Internet, do atendimento às especificações.

13.9. A falta de informações técnicas ou a incompatibilidade destas com as características especificadas implicará a desclassificação da proposta.

## 14. VISITA TÉCNICA

14.1. As LICITANTES poderão realizar visita técnica pelo período de três dias antecedentes a data a ser definida do procedimento licitatório de contratação.

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

14.3. A visita técnica deverá ocorrer por horário marcado, e será agendada com o Departamento de Tecnologia e Comunicação do Coren-RJ;

14.4. O agendamento de visita deverá ocorrer até 72 (setenta e duas) horas antes da data e horário de abertura do processo licitatório;

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

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

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



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

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

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

## **15. VIGÊNCIA E GARANTIA**

15.1. Os equipamentos adquiridos neste Certame terão garantia de 36 (trinta e seis) meses contados da data de assinatura do contrato.

15.2. O prazo de vigência do contrato será de 36 (trinta e seis) meses, contados a partir da assinatura do contrato, com eficácia após a publicação de seu extrato no Diário Oficial da União.

## **16. ACEITAÇÃO DEFINITIVA DOS SERVIÇOS**

16.1. A aceitação definitiva dos serviços deverá ser concedida mediante a entrega do serviço contratado no prazo estipulado no presente Termo de Referência, pelo fiscal do contrato a ser designado pelo COREN-RJ, conforme cronograma físico financeiro;

16.2. Para aceitação definitiva a CONTRATADA deverá realizar comprovação de atendimento a todos os itens, através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto à fornecedora do atestado de aptidão e ao fabricante para comprovar a autenticidade das informações prestada e da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento destes requisitos implicará na desclassificação da proposta.

## **17. FORMA DE PAGAMENTO**

17.1. O Pagamento será efetuado por intermédio de crédito em conta mediante apresentação de Nota Fiscal e após aceitação definitiva dos serviços que se dará com:

17.1.1. Entrega dos Equipamentos Lote 1 – Firewalls do Tipo A e Tipo B, Pontos de Acesso sem Fio,

17.1.2. Término da implantação da solução do Lote 1,

17.1.3. Treinamento da solução do Lote 1,

17.1.4. Entrega dos contatos para suporte durante o período de vigência do contrato 36 (trinta e seis) meses referente aos equipamentos do Lote 1

17.1.5. Apresentação do Termo de Avaliação de Prestação de Serviços emitido pelos fiscais do contrato, afirmando a finalização da execução dos serviços que compõem a solução de segurança do Lote 1;

17.1.6. Entrega dos Equipamentos Lote 2 – Switches PoE de Comunicação de Rede sem Fio PoE e Switches de Comunicação de Rede;

17.1.7. Término da implantação da solução do Lote 2,

17.1.8. Treinamento da solução do Lote 2,



17.1.9. Entrega dos contatos para suporte durante o período de vigência do contrato 36 (trinta e seis) meses referente aos equipamentos de Lote 2

17.1.10. Apresentação do Termo de Avaliação de Prestação de Serviços emitido pelos fiscais do contrato, afirmando a finalização da execução dos serviços que compõem a solução de segurança do Lote 2;

17.2. O COREN-RJ efetuará retenção na fonte de todos os tributos inerentes a prestação do serviço em questão;

17.3. O pagamento do valor global de cada solicitação se dará após a apresentação da fatura, que será aprovada e atestada pelo representante legal designado por este COREN-RJ, sendo também necessária a apresentação dos comprovantes de Certidão Negativa de Débito junto ao INSS (CND), Certidão Negativa de Débitos Trabalhistas (DNDT), Certificado de Regularidade junto ao FGTS e Certidão Negativa de Tributos Federais e Dívida Ativa da União.

17.4. O pagamento da fatura está condicionado à apresentação de Certidão Negativa de Débito junto ao INSS (CND), Certificado de Regularidade junto ao FGTS e Certidão Negativa de Tributos Federais e Dívida Ativa da União, sendo franqueado a contratante reter os pagamentos, rescindir o contrato, aplicar as demais sanções administrativas e promover a consignação judicial dos valores retidos acaso o contratado não regularize a sua situação fiscal no prazo de 20 (vinte) dias contados no recebimento de notificação expedida pela contratante para tanto.

## **18. FISCALIZAÇÃO**

18.1. Fica assegurado ao COREN-RJ o direito de acompanhar e fiscalizar os serviços prestados pela Contratada, com livre acesso aos locais de trabalho para obtenção de quaisquer esclarecimentos julgados necessários à execução dos trabalhos.

## **19. FONTE DE RECURSOS**

19.1. Origem dos Recursos – Recurso Próprio.

## **20. DO VALOR ESTIMADO**

20.1. O valor final do presente objeto será definido após a Cotação Prévia de Preços a ser realizada pela Setor de Compras em conjunto com a Comissão Permanente de Licitação – CPL.

## **21. COMPLEMENTAÇÃO**

21.1. Constituem-se em mandamentos e disposições gerais pertencentes a este termo de referência, os itens e subitens aqui descritos, possuindo todos a mesma importância, independentes ou não entre si, devendo ser observados e atendidos, não cabendo a nenhuma das partes reclamar o seu desconhecimento ou grau de relevância.

## **22. DISPOSIÇÕES FINAIS**

22.1. Seguirá em anexo ao instrumento do contrato.

**Aline Macedo Arza Lobo**

**Gerente do Departamento de Tecnologia da Informação e Comunicação/Coren-RJ**



**Coren<sup>RJ</sup>**  
Conselho Regional de Enfermagem do Rio de Janeiro

Processo n°: 1480/2016

Data: 05/12/2016

Folhas:

Rubrica:

## ANEXO II

### CRENCIAMENTO (MODELO)

(Papel Timbrado da Empresa)

NOME/RAZÃO SOCIAL

CNPJ/MF

ENDEREÇO

Pelo presente instrumento fica credenciado o Sr. \_\_\_\_\_, portador da Carteira de Identidade n° \_\_\_\_\_ e CPF sob n° \_\_\_\_\_, para representar a empresa \_\_\_\_\_, inscrita no CNPJ n° \_\_\_\_\_, na licitação na modalidade Pregão Presencial n° \_\_\_\_/\_\_\_\_ a ser realizado no dia \_\_\_\_/\_\_\_\_/\_\_\_\_ às \_\_\_\_\_, no **CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO**, com poderes específicos para tomar qualquer decisão relativa a todas as fases deste Pregão, podendo formular propostas de preços verbais, prestar esclarecimentos, receber notificação, interpor recurso e manifestar-se quanto a sua renúncia e eventual desistência.

Rio de Janeiro, de de 2017

---

Assinatura do Representante Legal



**ANEXO III**

**PROPOSTA DE PREÇOS**

(Papel Timbrado da Empresa)

**PREGÃO PRESENCIAL Nº \_\_\_\_\_/2017**

**NOME DA EMPRESA**

**Prazo:** 12 (doze) meses.

**Validade da Proposta:** 60 (sessenta) dias.

**Objeto:** Aquisição parcelada por registro de preços de solução de segurança de rede, conforme especificações do Termo de Referência (Anexo I).

Lote	Item	Descrição	Quantidade Prevista	Forma de Desembolso	Valor Unitário Estimado (R\$)	Valor Unitário Proposto (R\$)
1	1	Firewall de Borda no modo Cluster Ativo/Passivo – TIPO A	2	Único	31.863,33	
	2	Firewall Interno com Gerenciamento Centralizado (Stand Alone) – TIPO B	12	Único	8.910,00	
	3	Ponto de Acesso de Comunicação para Redes sem Fio	15	Único	4.413,33	
	4	Implantação da Solução de Segurança	1	Único	21.666,67	
	5	Treinamento da Solução de Segurança	1	Único	14.500,00	
	6	Suporte da Solução de Segurança	1	Único	21.666,67	
<b>Total LOTE 1</b>					<b>103.020,00</b>	
2	1	Switch PoE de Comunicação 24 portas para Redes sem Fio	4	Único	4.500,30	
	2	Switch de Comunicação 48 portas	6	Único	5.718,00	
	3	Implantação dos Switches de Comunicação de Rede	1	Único	12.566,67	
	4	Treinamento dos Switches de Comunicação de rede	1	Único	21.533,33	
	5	Suporte aos Switches de Comunicação de rede	1	Único	21.166,67	
<b>Total LOTE 2</b>					<b>65.484,97</b>	

**Valor por extenso:** \_\_\_\_\_

**Data da Cotação:** \_\_\_\_\_

\_\_\_\_\_  
Assinatura do Fornecedor



**ANEXO IV**

**MODELO DE DECLARAÇÃO PARA ME E EPP**

(Papel Timbrado da Empresa)

Declaro para os devidos fins que a empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, é microempresa/empresa de pequeno porte, nos termos do artigo 3º da Lei Complementar nº 123/2006, não estando incluída nas exclusões do § 4º do citado artigo.

Rio de Janeiro, de de 2017

---

Assinatura do representante legal



ANEXO V

**MODELO DE DECLARAÇÃO REFERENTE À HABILITAÇÃO**

(EM ATENDIMENTO AO INCISO VII DO ART. 4º DA LEI Nº 10.520/2002)

(Papel Timbrado da Empresa)

Declaro para os devidos fins que a empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, **cumpr** plenamente os requisitos exigidos para sua habilitação, conforme prescreve o inciso VII, do artigo 4º, da Lei 10.520, de 17 de julho de 2002, referente ao **PREGÃO PRESENCIAL Nº \_\_\_\_/\_\_\_\_**, estando ciente das penalidades aplicáveis nos casos de descumprimento.

Rio de Janeiro de de 2017

\_\_\_\_\_  
Assinatura do Representante Legal

**OBS.: ESTE DOCUMENTO DEVERÁ SER ENTREGUE NO ATO DO CREDENCIAMENTO, OU SEJA, FORA DOS ENVELOPES.**



**ANEXO VI**

**MODELO DE DECLARAÇÃO ART. 7º, XXXIII, DA CRFB**

(EM ATENDIMENTO AO ART. 27, INCISO V, DA LEI Nº 8.666/93 E ART. 7º, INCISO XXXIII, DA CRFB)

(Papel Timbrado da Empresa)

A empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, por intermédio do seu representante legal o(a) Sr(a) \_\_\_\_\_, portador(a) da Carteira de Identidade nº \_\_\_\_\_ e CPF sob nº \_\_\_\_\_, **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 (dezesesseis).**

**Ressalva:** emprega menor, a partir de 14 (quatorze) anos, na condição de aprendiz.

Rio de Janeiro, de de 2017

\_\_\_\_\_  
Assinatura do Representante Legal



**ANEXO VII**

**MODELO DE DECLARAÇÃO DE IDONEIDADE**

(EM CUMPRIMENTO DO ARTIGO 32, § 2º DA LEI Nº 8.666/93)

(Papel Timbrado da Empresa)

A empresa \_\_\_\_\_, inscrita no CNPJ sob o nº \_\_\_\_\_, DECLARA, sob as penas da lei, para fins do disposto no artigo 32, § 2º da Lei nº 8.666/93, por intermédio do seu representante legal, abaixo assinado, que não se encontra declarada inidônea para licitar ou contratar com órgãos da Administração Pública Federal, Estadual, Municipal e do Distrito Federal, bem como inexistente fato superveniente impeditivo de sua habilitação.

Rio de Janeiro, de de 2017

\_\_\_\_\_  
(Assinatura do representante legal)



**ANEXO VIII**

**(MODELO)**

**TERMO DE RECEBIMENTO DEFINITIVO**

A      [RAZÃO SOCIAL]     , inscrita no CNPJ/MF      [Nº do CNPJ]     , conforme a nota fiscal nº      de      /      /     , passados      dias da entrega, cumpriu os requisitos de especificação e de entrega do objeto, estabelecidos em Edital, anexos e proposta do certame licitatório do Conselho Regional de Enfermagem do Rio de Janeiro, Pregão Presencial-SRP nº     .

Rio de Janeiro,      de      de 2017

---

Chefe do Almoxarifado



**ANEXO IX**

**MINUTA DA ATA DE REGISTRO DE PREÇOS  
CONSELHO REGIONAL DE ENFERMAGEM  
ATA DE REGISTRO DE PREÇOS**

**Pregão Eletrônico de Registro de Preços N° \_\_\_\_\_/2017**

**Órgão Gerenciador: Conselho Regional de Enfermagem do Rio de Janeiro**

**UASG: 389337**

Compromisso celebrado entre o **CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO**, situado na Avenida Presidente Vargas, n° 502, 5° andar, Centro, Rio de Janeiro/RJ, doravante denominada \_\_\_\_\_, representada neste ato pelo sua Presidente Sra. MARIA ANTONIETA RUBIO TYRRELL, brasileira, casada, portadora da identidade profissional COREN/RJ n° 9.719, inscrita no CPF sob o n° \_\_\_\_\_, e seu primeiro-tesoureiro \_\_\_\_\_, (qualificação), portador da cédula profissional COREN/RJ n° \_\_\_\_\_, e inscrito no CPF sob o n° \_\_\_\_\_, ambos empossados pela Decisão COFEN N° 190/2014, se 10 de outubro de 2014 e Decisão COREN/RJ n° 1942-A/2014, de 28 de outubro de 2014, e a empresa \_\_\_\_\_, inscrita no CNPJ sob n° \_\_\_\_\_ estabelecida na \_\_\_\_\_, neste ato representada pelo Sr. \_\_\_\_\_ (profissão), inscrito no CPF sob o n° \_\_\_\_\_, e no RG n° \_\_\_\_\_, expedida pelo \_\_\_\_\_, residente e domiciliado na \_\_\_\_\_.

O presente compromisso tem seu fundamento e finalidade na consecução do objeto descrito abaixo, constante do processo administrativo 183/2015, e Edital n° 003/2015 regendo-se o mesmo pelo Decreto Federal 3.555 de 08/08/00 e respectivas alterações, pela Lei Federal n° 10.520 de 17/07/02, pelas Leis Complementares n° 101, de 2000 (Lei de Responsabilidade Fiscal) e n° 123 de 2006 e em especial o Decreto n° 7.892/2013, todos com aplicação subsidiária da Lei Federal n° 8.666 de 21/06/93 e pela legislação pertinente, assim como pelas condições do Edital Referido, pelos termos da proposta e pelas cláusulas a seguir expressas, definidoras dos direitos, obrigações e responsabilidades das partes.

**CLÁUSULA PRIMEIRA - DO OBJETO E DO PREÇO**

O presente compromisso tem por objeto o Registro de Preços para aquisição de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o Coren-RJ e suas subseções, compreendendo o fornecimento, a implantação, o suporte técnico, a garantia e o treinamento do: Firewall de Borda no modo Cluster Ativo/Passivo – TIPO A, Sistema de Firewall Interno com Gerenciamento Centralizado (Stand Alone) – TIPO B, os dois firewalls deverão suportar Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall), Ponto de Acesso de Comunicação para Redes sem Fio e Switch PoE, conforme especificações constantes dos Anexos do Termo de Referência.

**PARÁGRAFO PRIMEIRO.** As quantidades acima indicadas não poderão sofrer acréscimos, conforme disposto no §1° do artigo 12 do Decreto n° 7.892/2013.

**PARÁGRAFO SEGUNDO.** O preço unitário para cada item englobará todas as despesas relativas ao objeto deste compromisso, bem como os respectivos custos diretos e indiretos, incluindo transporte e entrega no local indicado pelo COREN/RJ, seguro, tributos, remunerações, despesas fiscais e financeiras



e quaisquer outras necessárias ao cumprimento do objeto desta Ata. Nenhuma reivindicação adicional de pagamento ou reajustamento de preços será considerada.

## **CLÁUSULA SEGUNDA - DA CONTRATAÇÃO E DOS PRAZOS**

As contratações dos fornecimentos dos itens com preços registrados serão formalizados pelo Órgão Gestor da presente Ata de Registro de Preços, ou pelos que vierem a aderir, através da entrega da Nota de Empenho ou Solicitação de Fornecimento a Compromitente.

**PARÁGRAFO ÚNICO.** O prazo de validade desta Ata de Registro de Preço é improrrogável e será de 12 (doze) meses, contados a partir de sua assinatura.

## **CLAUSULA TERCEIRA - DA ENTREGA E RECEBIMENTO**

As entregas deverão ser efetuadas na forma prevista no Termo de Referência, atendendo às requisições de fornecimento que serão emitidas especificando local, dia e hora para entregas, com utilização de pessoal para descarregamento sob a responsabilidade da Contratada, devendo os materiais estar em perfeitas condições para serem utilizados, e as embalagens não danificadas.

**PARÁGRAFO PRIMEIRO.** Os fornecimentos deverão seguir os locais e horários previamente definidos na Nota de Empenho ou na Solicitação de fornecimento, sendo certo que poderão ocorrer em qualquer dia e horário da semana seguindo critérios de melhor execução e disponibilização dos espaços.

**PARÁGRAFO SEGUNDO.** Os produtos deverão ser entregues acondicionados adequadamente, quando for o caso, com rotulo contendo a descrição, a data de fabricação e validade, o registro no órgão de fiscalização e outras informações necessárias, e estar acompanhado da nota fiscal correspondente, devidamente preenchida.

**PARÁGRAFO TERCEIRO.** A descrição dos produtos deverá ser seguida a risca. Qualquer alteração deverá ser consultada antes da entrega, não sendo obrigado o Contratante a acatá-la.

**PARÁGRAFO QUARTO.** O material solicitado será recebido provisoriamente. Após o prazo de 5 (cinco) dias úteis, verificada compatibilidade do material com o Edital e Proposta, bem como sua qualidade será recebido definitivamente, emitindo-se o Termo de Recebimento definitivo.

**PARÁGRAFO QUINTO.** Constatadas irregularidades na entrega dos objetos, a Administração poderá:

- a) Se disser respeito à especificação, rejeitá-lo no todo ou em parte, determinando sua substituição ou complementação, ou rescindindo a contratação, sem prejuízo das penalidades cabíveis;
- b) Na hipótese de substituição, a licitante deverá fazê-la em conformidade com a indicação da Administração, no prazo máximo de 03 (três) dias úteis contados da notificação por escrito, mantidos os preços inicialmente registrados;
- c) Na hipótese do parágrafo anterior, o prazo de 5 (cinco) dias será interrompido até que sejam sanadas as irregularidades, recomeçando seu cômputo apenas quando da efetivação da nova entrega dos materiais substituídos ou complementados;

**PARÁGRAFO SEXTO.** A entrega do material substituído ou complementado dar-se-á novamente de forma provisória, a fim de que seja novamente aferida a sua compatibilidade com os termos do presente Edital. Verificando-se que a nova entrega está em termos, será emitido Termo de Recebimento Definitivo.

**PARÁGRAFO SÉTIMO.** Caso a nova entrega ainda se verifique fora dos padrões do Edital, a Administração optará entre notificar novamente o Compromitente ou declarar o inadimplemento contratual, com a aplicação das sanções pertinentes.



#### **CLAUSULA QUARTA - DA VALIDADE DO PRODUTO**

O produto requerido, se for o caso, deverá possuir prazo de validade de no mínimo 12 (doze) meses.

**PARÁGRAFO PRIMEIRO.** Durante o prazo de validade, o Compromitente obriga-se a substituir ou reparar, às suas expensas, qualquer material que apresente defeito que não seja decorrente do desgaste natural ou do incorreto manuseio.

**PARÁGRAFO SEGUNDO.** Incumbe ao Compromitente o ônus da prova da origem do defeito.

#### **CLAUSULA QUINTA - DO PAGAMENTO**

Os valores relativos aos fornecimentos contratados serão pagos de acordo com a quantidade e o valor dos itens efetivamente fornecidos, condicionados a apresentação das notas fiscais/faturas, as quais deverão ser devidamente atestadas pelo funcionário do Conselho Regional de Enfermagem do Rio de Janeiro responsável pela fiscalização deste Registro.

**PARÁGRAFO PRIMEIRO.** Os pagamentos serão efetuados em moeda corrente nacional, através de credito na conta corrente da Contratada, Agencia n° \_\_\_\_\_, Conta Corrente n°. \_\_\_\_\_ Banco \_\_\_\_\_ até o 30° (trigésimo) dia subsequente ao recebimento definitivo dos itens fornecidos, sempre de acordo com a ordem cronológica de sua exigibilidade.

**PARÁGRAFO SEGUNDO.** A Nota Fiscal apresentada para pagamento deverá ser do estabelecimento que apresentou a proposta vencedora da Licitação, e isento de erros.

**PARÁGRAFO TERCEIRO.** Junto com a Nota Fiscal o Contratado deverá estar encaminhar impreterivelmente os seguintes documentos: Certidão Negativa de Débitos – relativos às contribuições previdenciárias e às de terceiros, Certidão Conjunta de Débitos – relativos aos tributos federais da dívida ativa da União, Certificado de Regularidade do FGTS e cópia da nota de empenho.

**PARÁGRAFO QUARTO.** Caso se faz necessária à reapresentação de qualquer fatura por culpa da Compromitente, o prazo de 30 (trinta) dias ficará suspenso, prosseguindo a sua contagem a partir da data da respectiva apresentação.

**PARÁGRAFO QUINTO.** Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuído a Compromitente, serão acrescidos da taxa de 1% (um por cento) ao mês, calculada *pro rata die* entre o 31° dia da data do adimplemento da obrigação e a data do efetivo pagamento.

**PARÁGRAFO SEXTO.** Nenhum pagamento será efetuado enquanto pendente de liquidação, pelo Compromitente, qualquer obrigação financeira que lhe for imposta, em virtude de penalidade ou inadimplência, sem que isso gere direito a acréscimos de qualquer natureza.

**PARÁGRAFO SÉTIMO.** Do montante devido ao Compromitente poderão ser deduzidos os valores correspondentes a multas e/ou indenizações impostas pelo COREN/RJ

#### **CLAUSULA SEXTA - DOS DIREITOS E DAS OBRIGAÇÕES**

##### **1. DO DIREITO**

##### **1.1. DO COREN/RJ**

1.1. Contratar se necessário o objeto desta ata de Registro de Preços.

##### **1.2. DA COMPROMITENTE**

1.2.1. Ser contratada se a Administração utilizar o Registro de Preços, ou, se preferido em igualdade de condições, no caso de outra licitação realizada para o mesmo objeto desse Registro de Preços.

##### **2. DAS OBRIGAÇÕES**



## 2.1. DO COREN/RJ

- a) Realizar os pagamentos devidos à CONTRATADA nas condições estabelecidas no Instrumento Contratual;
- b) Fornecer à CONTRATADA documentos, informações e demais elementos que possuir, necessários à boa execução do presente contrato;
- c) Acompanhar e fiscalizar a execução dos serviços, registrar as ocorrências e eventuais deficiências relacionadas com a execução, sob os aspectos quantitativos e qualitativos e comunicar as ocorrências de quaisquer fatos que exijam medidas corretivas por parte da CONTRATADA;
- d) Informar à CONTRATADA, por escrito, as razões que motivaram eventual rejeição dos serviços contratados e/ou cancelamento;

## 2.2. DA COMPROMITENTE

- a) Entregar o material no prazo, no local e nas condições exigidas neste Termo de Referência;
- b) Juntamente com a entrega do material, emitir Nota Fiscal com a mesma descrição constante na Nota de Empenho;
- c) A Empresa contratada também se responsabilizará por perdas e danos eventualmente causados por seus técnicos ou empregados, a bens e/ou equipamentos de propriedade da CONTRATANTE ou TERCEIROS durante a entrega dos materiais.
- d) Efetuar a troca ou substituição do material que não esteja conforme a descrição deste Projeto Básico ou cuja qualidade não atenda aos requisitos mínimos de uso.
- e) **5.** Os itens cujas unidades de medida sejam embalagem (caixa ou pacote) e que contenham mais de uma unidade por invólucro devem ser entregues obedecendo à unidade de medida registrada e tendo em seu conteúdo a quantidade mínima da especificação, não sendo recebidos itens pelo somatório de suas unidades ou com quantidade unitária à menor da especificada.

## CLAUSULA SÉTIMA - DA REVOGAÇÃO OU SUSPENSÃO DO REGISTRO DE PREÇOS

O preço registrado poderá ser revogado pelo COREN/RJ quando:

- a) A Compromitente não cumprir as exigências desta Ata e do instrumento convocatório;
- b) Ocorrer qualquer das hipóteses de inexecução total ou parcial das obrigações decorrentes desta Ata de Registro de Preços;
- c) Os preços registrados apresentarem-se superiores aos do mercado;
- d) A compromitente der causa a rescisão administrativa, por um dos motivos elencados no art. 78 e seus inciso da Lei nº 8.666/93;
- e) Por razão de interesse público, devidamente justificado pela Administração.

**PARÁGRAFO PRIMEIRO.** O Registro de Preços poderá ser suspenso a pedido da Compromitente mediante requerimento por escrito, sujeito a aprovação do COREN/RJ, quando ficar comprovada a impossibilidade definitiva ou temporária de cumprir as exigências da licitação que deu origem ao Registro de Preços.

**PARÁGRAFO SEGUNDO.** O pedido de suspensão efetuado pela Compromitente deverá ser feito por escrito, por meio de correspondência com aviso de recebimento, com antecedência de no mínimo 30 (trinta) dias, sendo facultada ao COREN/RJ a aplicação das penalidades previstas no Edital e em seus anexos.

## CLÁUSULA OITAVA - DAS PENALIDADES E DAS MULTAS



O adjudicatário ou contratado inadimplente está sujeito às penalidades previstas no artigo 87, da Lei n° 8.666/93 e no artigo 7° da Lei 10.520, bem como aquelas previstas no item 22 do Edital, assegurando o contraditório e a ampla defesa.

#### **CLÁUSULA NONA - DA EFICÁCIA**

A presente Ata de Registro de Preços somente terá eficácia depois de publicado o respectivo extrato no Diário Oficial do Estado do Rio de Janeiro.

#### **CLÁUSULA DÉCIMA - DAS DISPOSIÇÕES GERAIS**

Fica eleito o Foro da Justiça Federal, Seção Judiciária do Rio de Janeiro, para dirimir dúvidas ou questões oriundas do presente instrumento.

E, por estarem as partes justas e compromissadas, assinam a presente Ata em 03 (três) vias, de igual teor, na presença das testemunhas abaixo arroladas.

Rio de Janeiro, \_\_\_\_\_ 2016

**PRESIDENTE DO CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO**

**PRIMEIRO TESOUREIRO DO CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO**

\_\_\_\_\_  
**COMPROMITENTE**

**TESTEMUNHAS:**

1. \_\_\_\_\_

CPF n°

2. \_\_\_\_\_

CPF n°



**ANEXO X**

**MODELO DE SOLICITAÇÃO DE FORNECIMENTO**

**SOLICITAÇÃO DE FORNECIMENTO Nº \_\_\_\_ /2016**

**FORNECEDOR:** \_\_\_\_\_

**1. DO OBJETO**

A presente Solicitação de Fornecimento tem por objeto aquisição parcelada aquisição parcelada por registro de preços de solução de rede, conforme especificações do Termo de Referência (Anexo I) e na proposta da contratada, referentes ao Pregão Presencial por Registro de Preços nº \_\_\_\_ /2016.

Item	Especificação	Unidade	Quantidade	Valor Unitário	Valor Total	Percentual Utilizado

**2. DO PRAZO E DO LOCAL DE ENTREGA**

**2.1.** O prazo máximo de entrega do material é de \_\_\_\_ (\_\_\_\_\_) dias, a contar do recebimento da presente solicitação e da Nota de Empenho, sob pena de aplicação das sanções previstas na Ata de Registro de Preços e no Edital nº \_\_\_\_ /2017.

**2.2.** As entregas deverão ser realizadas em \_\_\_\_ / \_\_\_\_ / \_\_\_\_ na sede do Conselho no 6º andar da Avenida Presidente Vargas, 502, no horário das 9h às 11h ou no horário de 14h às 16h;

**3. DO PREÇO**

**3.1.** O Conselho Regional de Enfermagem do Rio de Janeiro pagará à contratada o valor total de R\$ \_\_\_\_ (\_\_\_\_\_), pelos bens nas quantidades descritas acima.

**3.2.** Estão incluídos no preço proposto a incidência tributária e demais encargos como materiais, mão de obra, equipamentos, licenças, impostos, taxas, emolumentos, transportes, embalagens, seguro, enfim todas as despesas pertinentes ao fornecimento.

Rio de Janeiro, \_\_\_\_ / \_\_\_\_ / \_\_\_\_

(Nome e cargo do servidor – Setor Requisitante)



**ANEXO XI**

**DESCRIÇÃO DOS MATERIAIS, QUANTITATIVOS E VALORES DE REFERÊNCIA**

<b>Lote</b>	<b>Item</b>	<b>Descrição</b>	<b>Valor Unitário Estimado (R\$)</b>	<b>Valor Unitário Proposto (R\$)</b>
1	1	Firewall de Borda no modo Cluster Ativo/Passivo – TIPO A		
	2	Firewall Interno com Gerenciamento Centralizado (Stand Alone) – TIPO B		
	3	Ponto de Acesso de Comunicação para Redes sem Fio		
	4	Implantação da Solução de Segurança		
	5	Treinamento da Solução de Segurança		
	6	Suporte da Solução de Segurança		
2	1	Switch PoE de Comunicação 24 portas para Redes sem Fio		
	2	Switch de Comunicação 48 portas		
	3	Implantação dos Switches de Comunicação de Rede		
	4	Treinamento dos Switches de Comunicação de rede		
	5	Suporte aos Switches de Comunicação de rede		



## ANEXO XII

### DESCRIÇÃO DOS MATERIAIS, QUANTITATIVOS E VALORES DE REFERÊNCIA

#### MINUTA DE CONTRATO

**CONTRATO DE AQUISIÇÃO DE SOLUÇÃO DE SEGURANÇA DA INFORMAÇÃO E OUTRAS AVENÇAS QUE ENTRE SI CELEBRAM O CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO/COREN/RJ E A EMPRESA \_\_\_\_\_ (PROCESSO Nº \_\_\_\_\_).**

O **CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO – COREN-RJ**, autarquia federal fiscalizadora do exercício profissional de enfermagem no âmbito do Estado do Rio de Janeiro, ex vi da Lei Federal n.º 5.905/73, com sede na Av. Presidente Vargas, n.º 502, 5º andar, Centro, Rio de Janeiro/RJ, CEP: 20.071.000, CNPJ n.º 27.149.095/001-66, doravante denominado **CONTRATANTE**, representado neste ato por sua Presidente, **Dr.ª MARIA ANTONIETA RUBIO TYRRELL**, brasileira, casada, portador de identidade profissional COREN/RJ n.º 9.719, e pelo Primeiro Tesoureiro, **Sr. PAULO MURILO DE PAIVA**, brasileiro, \_\_\_\_\_ [qualificação], ambos empossados pela **Decisão COFEN n.º 190/2014 de 10º de outubro de 2014 e Decisão COREN RJ n.º 1942-A/2014 de 28 de outubro de 2014**, doravante denominado **CONTRATANTE**, de outro lado, e a empresa [IDENTIFICAR A EMPRESA], inscrita no CNPJ sob o n.º \_\_\_\_\_ [CITAR CNPJ], doravante denominada **CONTRATADA**, neste ato representada por \_\_\_\_\_ [IDENTIFICAR E QUALIFICAR O REPRESENTANTE], resolvem celebrar o presente **CONTRATO**, tendo sua celebração justificada e autorizada nos autos do processo administrativo n.º \_\_\_\_\_, e se regerá por toda a legislação aplicável à espécie, especialmente as normas contidas na Lei Federal n.º 10.520/2002, no que couber a Lei Federal n.º 8.666/1993 e suas alterações e no termo de Referência, que passa a ser parte integrante do presente instrumento, observando-se, ainda, as cláusulas e condições a seguir estabelecidas.

#### CLÁUSULA PRIMEIRA – DO OBJETO

O presente **CONTRATO** tem por objeto a aquisição de Solução de Segurança da Informação e contratação de empresas especializadas na prestação de Serviços de Segurança de Perímetro com soluções em alta disponibilidade para o Coren-RJ e suas subseções, compreendendo o fornecimento, a implantação, o suporte técnico, a garantia e o treinamento do: Firewall de Borda no modo Cluster Ativo/Passivo – TIPO A, Sistema de Firewall Interno com Gerenciamento Centralizado (Stand Alone) – TIPO B, os dois firewalls deverão suportar Prevenção Contra Intrusão (IPS), Filtro de Conteúdo Web (Webfilter), Antivírus de Gateway, Firewall de Aplicação Web (Web Application Firewall), Ponto de Acesso de Comunicação



para Redes sem Fio e Switch PoE, conforme especificações constantes dos Anexos que fazem parte deste Termo de Referência. Os serviços aqui descritos serão prestados no Anexo I do COREN/RJ, localizado à Avenida Presidente Vargas, n.º 502, 3.º, 4.º, 5.º e 6.º Andares, Centro, Rio de Janeiro-RJ.

**PARÁGRAFO ÚNICO.** A CONTRATADA, na execução do presente contrato, deverá prestar os serviços conforme as especificações contidas no Termo de Referência, que faz parte do presente contrato.

### **CLÁUSULA SEGUNDA – DO PRAZO E DA EXECUÇÃO**

O prazo de vigência do contrato será de \_\_\_\_ (\_\_\_\_\_) meses, contados a partir de sua assinatura.

**PARÁGRAFO PRIMEIRO.** O prazo contratual poderá ser prorrogado, observando-se o limite previsto no art. 57, II, da Lei n.º 8.666/93, desde que a proposta da CONTRATADA seja mais vantajosa para o CONTRATANTE.

### **CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DO CONTRATANTE**

Durante a vigência deste CONTRATO o CONTRATANTE obriga-se a cumprir fielmente o estipulado nas CLÁUSULAS deste Instrumento, em especial:

- a. Oferecer todas as informações necessárias para que a CONTRATADA possa executar o contrato dentro das especificações recomendadas, além de toda infraestrutura física e elétrica para instalação dos equipamentos;
- b. Fornecer, a qualquer tempo, mediante solicitação escrita da CONTRATADA, informações adicionais, retirar dúvidas e orientá-la em todos os casos omissos que ocorrerem;
- c. Receber os empregados da CONTRATADA, devidamente credenciados, para instalação e manutenção dos equipamentos, tomando as providências administrativas que garantam o livre desempenho de tais atividades;
- d. Comunicar à CONTRATADA, o mais prontamente possível, qualquer anormalidade observada na prestação dos serviços;
- e. Atestar a Nota Fiscal correspondente ao mês de execução dos serviços prestados;
- f. Efetuar o Pagamento dos serviços prestados efetivamente, mediante Nota Fiscal devidamente atestada;
- g. Designar gestor para acompanhamento e fiscalização do contrato, que deverá atestar a execução do mesmo;
- h. Aplicar as penalidades, quando cabíveis.

**PARÁGRAFO ÚNICO.** As atribuições do Fiscal do Contrato, devidamente designado para este fim, além daquelas naturalmente inerentes ao encargo, encontram-se descritas no Termo de Referência.

### **CLÁUSULA QUARTA – DAS OBRIGAÇÕES DA CONTRATADA**



Durante a vigência deste CONTRATO a CONTRATADA obriga-se a cumprir fielmente o estipulado nas CLÁUSULAS deste Instrumento, em especial:

- a. Fornecer os equipamentos e prestar os serviços de acordo com as especificações constantes no Termo de Referência;
- b. Iniciar e concluir os serviços em prazo não superior ao máximo estipulado no presente Contrato e no Termo de Referência;
- c. Disponibilizar manutenção e gerenciamento dos equipamentos e da rede envolvida;
- d. Manter durante a vigência do Contrato as condições de habilitação para contratar com a Administração Pública, apresentando sempre que exigidos os comprovantes de inexistência de débitos federais, estaduais, municipais, FGTS, INSS e trabalhistas;
- e. Comunicar por escrito quando verificar condições inadequadas para a execução do CONTRATO, apresentando justificativas que serão objeto de apreciação pelo CONTRATANTE;
- f. Assegurar ao CONTRATANTE o direito de fiscalizar, sustar, recusar, mandar refazer qualquer serviço e/ou fornecimento que não esteja de acordo com as normas ou especificações técnicas, bem como os quais tenha dado causa;
- g. Prestar todos os esclarecimentos que lhes forem solicitados pelo CONTRATANTE, atendendo prontamente às reclamações;

#### **CLÁUSULA QUINTA – DA DOTAÇÃO ORÇAMENTÁRIA**

As despesas com a execução do presente contrato correrão à conta das seguintes dotações orçamentárias, para o corrente exercício de \_\_\_\_\_, assim classificados:

Natureza das Despesas:

Fonte de Recurso:

Nota de Empenho:

**PARÁGRAFO ÚNICO.** As despesas relativas aos exercícios subsequentes correrão por conta das dotações orçamentárias respectivas, devendo ser empenhadas no início de cada exercício.

#### **CLÁUSULA SEXTA – DA VIGÊNCIA, DO VALOR E DO REAJUSTE**

O presente contrato tem prazo de vigência de 12 (doze) meses.

O valor mensal do contrato é R\$ \_\_\_\_\_ (\_\_\_\_\_), totalizando-se R\$ \_\_\_\_\_ (\_\_\_\_\_) no ano.

O Contrato será reajustado pela aplicação do Índice Geral de Preços – IGP-10 ou outro que venha a substituí-lo.

**PARÁGRAFO PRIMEIRO:** A periodicidade de aplicação do índice de correção é de 12 (doze) meses, cujo aniversário é contado da data limite para apresentação da proposta no processo licitatório.

**PARÁGRAFO SEGUNDO:** O Contrato poderá ser renegociado a qualquer tempo se houver desequilíbrio econômico-financeiro, na forma da legislação vigente.



## **CLÁUSULA SÉTIMA – DA EXECUÇÃO, DO RECEBIMENTO E DA FISCALIZAÇÃO DO CONTRATO**

O contrato deverá ser executado de acordo com as cláusulas avençadas, nos termos do instrumento convocatório e da legislação vigente, respondendo o inadimplente pelas consequências da inexecução total ou parcial.

**PARÁGRAFO PRIMEIRO.** A execução do contrato será acompanhada e fiscalizada por 1 (um) representante do CONTRATANTE especialmente designado pelo Presidente do contratante mediante edição de portaria.

**PARÁGRAFO SEGUNDO.** O objeto será recebido na forma prevista no art. 73 da Lei nº 8.666/1993, dispensada o recebimento provisório nas hipóteses previstas no art. 74 da mesma Lei.

**PARÁGRAFO TERCEIRO.** A CONTRATADA declara, antecipadamente, aceitar todas as condições, métodos e processos de inspeção, verificação e controle adotados pela fiscalização, obrigando-se a fornecer todos os dados, elementos, explicações, esclarecimentos e comunicações de que esta necessitar e que forem julgados necessários ao desempenho de suas atividades.

**PARÁGRAFO QUARTO.** A instituição e a atuação da fiscalização não exclui ou atenua a responsabilidade da CONTRATADA, nem a exime de manter fiscalização própria.

## **CLÁUSULA OITAVA – DA RESPONSABILIDADE**

A CONTRATADA é responsável por danos causados ao CONTRATANTE ou a terceiros, decorrentes de culpa ou dolo na execução do contrato, não excluída ou reduzida essa responsabilidade pela presença de fiscalização ou pelo acompanhamento da execução por órgão da Administração.

**PARÁGRAFO ÚNICO.** A CONTRATADA é responsável por encargos trabalhistas, inclusive decorrentes de acordos, dissídios e convenções coletivas, previdenciários, fiscais e comerciais oriundos da execução do contrato, podendo o CONTRATANTE, a qualquer tempo, mediante prévia solicitação, exigir a comprovação do cumprimento de tais encargos, como condição do pagamento dos créditos da CONTRATADA.

## **CLÁUSULA NONA – CONDIÇÕES DE PAGAMENTO**

O CONTRATANTE deverá pagar à CONTRATADA o valor mensal de até R\$ \_\_\_\_\_ (\_\_\_\_\_), sendo o pagamento efetuado em conta corrente de titularidade da CONTRATADA ou mediante boleto de cobrança emitido pela CONTRATADA.

**PARÁGRAFO PRIMEIRO.** A consulta relativa à regularidade fiscal, exigida quando da habilitação, será feita previamente ao pagamento, devendo seu resultado ser juntado aos autos do processo próprio e ficando o efetivo pagamento a ela condicionado.

**PARÁGRAFO SEGUNDO.** A CONTRATADA deverá encaminhar a nota fiscal para pagamento, em até \_\_\_\_ (\_\_\_\_\_) dias da efetiva prestação dos serviços.



**PARÁGRAFO TERCEIRO.** O prazo para pagamento é de 10 (dez) dias úteis após a prestação do serviço do mês de referência e do atesto da Nota Fiscal, considerando a certificação da execução do objeto e das obrigações contratuais pela CONTRATADA.

**PARÁGRAFO QUARTO.** Caso se faça necessária a reapresentação de qualquer nota fiscal por culpa da CONTRATADA, o prazo de 30 (trinta) dias reiniciar-se-á a contar da data da respectiva reapresentação.

**PARÁGRAFO QUINTO.** Os pagamentos eventualmente realizados com atraso, desde que não decorram de ato ou fato atribuível à CONTRATADA, serão acrescidos da taxa de 1% (um por cento) ao mês, calculada pro rata die entre o 11º dia da data do adimplemento da obrigação e a data do efetivo pagamentos.

## **CLÁUSULA DÉCIMA – DA ALTERAÇÃO DO CONTRATO**

O Contrato poderá ser modificado pelo CONTRATANTE, com as devidas justificativas, na forma prevista no artigo 65 e §§ da Lei n.º 8.666/1993, mediante a assinatura do respectivo Termo Aditivo a ser publicado.

## **CLÁUSULA DÉCIMA PRIMEIRA – DAS SANÇÕES ADMINISTRATIVAS E DEMAIS PENALIDADES**

Sem prejuízo de indenização por perdas e danos, cabível nos termos do Código Civil, a Administração poderá impor à licitante, adjudicatária ou contratada, pelo descumprimento total ou parcial das obrigações a que esteja sujeita, as sanções previstas no artigo 7º da Lei Federal nº 10.520/2002 e no artigo 87 da Lei nº 8.666/1993.

**PARÁGRAFO PRIMEIRO.** O atraso injustificado na execução do serviço sujeitará a CONTRATADA à multa de mora, fixada no edital. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a Adjudicatária pela diferença, que será descontada dos pagamentos eventualmente devidos pela Administração ou cobrada judicialmente.

**PARÁGRAFO SEGUNDO.** Pela inexecução total ou parcial da obrigação assumida, a Administração poderá aplicar as seguintes sanções, garantida prévia defesa:

- a) advertência;
- b) multa de mora de até 1% (um por cento) por dia útil sobre o valor do contrato, até o período máximo de 30 (trinta) dias úteis;
- c) multa de 20% (vinte por cento) sobre o valor do contrato, após esgotado o prazo fixado no subitem anterior;
- d) suspensão temporária de participação em licitações, ou impedimento de contratar com a Administração Pública, por prazo não superior a 2 (dois) anos;
- e) declaração de inidoneidade para licitar ou contratar com a Administração Pública, pelo prazo de até 5 (cinco) anos.



**PARÁGRAFO TERCEIRO.** As sanções previstas nas alíneas a, d e e poderão ser aplicadas juntamente com aquelas previstas nas alíneas b e c e não excluem a possibilidade de rescisão administrativa do contrato, garantida a defesa prévia ao interessado.

**PARÁGRAFO QUARTO.** As sanções estabelecidas nas alíneas d e e são da competência da Presidência do COREN/RJ.

**PARÁGRAFO QUINTO.** As sanções previstas nas alíneas d e e poderão também ser aplicadas às licitantes que, em outras contratações com a Administração Pública de qualquer nível federativo ou com autarquias, fundações, empresas públicas ou sociedade de economia mista tenham:

- a) sofrido condenação definitiva por praticarem, por meios dolosos, fraudes fiscais no recolhimento de quaisquer tributos;
- b) praticados atos ilícitos, visando a frustrar os objetivos da licitação;
- c) demonstrado não possuir idoneidade para contratar com a Administração, em virtude de outros atos ilícitos praticados.

#### **CLÁUSULA DÉCIMA SEGUNDA – DA RESCISÃO UNILATERAL DO CONTRATO**

O presente contrato poderá ser rescindido nos termos dos artigos 77 a 80 da Lei n.º 8.666/1993, por ato unilateral do CONTRATANTE, pela inexecução total ou parcial de suas cláusulas e condições ou ainda por interesse público superveniente.

**PARÁGRAFO PRIMEIRO.** Os casos de rescisão contratual serão formalmente motivados nos autos do processo administrativo, assegurado a CONTRATADA o direito ao contraditório e a prévia e ampla defesa.

**PARÁGRAFO SEGUNDO.** A declaração de rescisão deste contrato, independentemente da prévia notificação judicial ou extrajudicial, produz efeitos em relação a CONTRATADA a partir da sua ciência e a terceiros a partir da publicação em Diário Oficial.

#### **CLÁUSULA DÉCIMA TERCEIRA – DO RECURSO AO JUDICIÁRIO**

As importâncias decorrentes de quaisquer penalidades impostas à CONTRATADA, inclusive perdas e danos ou prejuízos que a execução do contrato tenha acarretado, quando não comportarem cobrança amigável, serão cobrados judicialmente, caso sejam superiores à garantia prestada, se for o caso, ou aos créditos que a CONTRATADA tenha em face do CONTRATANTE.

**PARÁGRAFO ÚNICO.** Caso o CONTRATANTE tenha de recorrer ou comparecer a juízo para haver o que lhe for devido, a CONTRATADA ficará sujeita ao pagamento, além do principal do débito, da pena convencional de 10% (dez por cento) sobre o valor do litígio, dos juros de mora de 1% (um por cento) ao mês, despesas de processo e honorários de advogado, estes fixados, desde logo, em 20% (vinte por cento) sobre o valor em litígio.

#### **CLÁUSULA DÉCIMA QUARTA – DA CESSÃO OU TRANSFERÊNCIA E SUBCONTRATAÇÃO**



O presente contrato não poderá ser objeto de cessão, transferência ou subcontratação, no todo ou em parte, a não ser com prévio e expresso consentimento do CONTRATANTE e sempre mediante instrumento próprio, devidamente motivado, a ser publicado.

**PARÁGRAFO PRIMEIRO.** Na hipótese de anuência do CONTRATANTE, o cessionário ficará sub-rogado em todos os direitos e obrigações do cedente e deverá atender a todos os requisitos de habilitação estabelecidos na legislação específica.

**PARÁGRAFO SEGUNDO.** Em caso de subcontratação, a CONTRATADA permanecerá, integral e exclusivamente, a única responsável, tanto em relação ao CONTRATANTE, como perante terceiros, assim como pelos serviços porventura subcontratados, podendo, inclusive, o CONTRATANTE exigir a substituição da empresa subcontratada, caso esta não esteja executando os serviços de acordo com os dispositivos contratuais.

#### **CLÁUSULA DÉCIMA QUINTA – EXCEÇÃO DE INADIMPLEMENTO**

Constitui cláusula essencial do presente contrato, de observância obrigatória por parte da CONTRATADA, a impossibilidade, perante o CONTRATANTE, de opor, administrativamente, exceção de inadimplemento, como fundamento para a interrupção unilateral do serviço.

**PARÁGRAFO ÚNICO.** A suspensão do contrato, a que se refere o art. 78, XIV e XV da Lei n.º 8.666/1993, se não for objeto de prévia autorização, deverá ser requerida judicialmente, mediante demonstração dos riscos decorrentes da continuidade da execução do contrato, sendo vedada sua suspensão por decisão unilateral da CONTRATADA.

#### **CLÁUSULA DÉCIMA SEXTA – CONDIÇÕES DE HABILITAÇÃO**

A CONTRATADA se obriga a manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

#### **CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO E CONTROLE DO CONTRATO**

Após a assinatura do contrato deverá seu extrato ser publicado, no prazo de 20 (vinte) dias, no Diário Oficial da União, correndo os encargos por conta da CONTRATANTE.

**PARÁGRAFO ÚNICO.** O extrato da publicação deve conter a identificação do instrumento, partes, objeto, prazo, valor, número do empenho, fundamento legal do ato e nº. do processo administrativo.

#### **CLÁUSULA DÉCIMA OITAVA – DA CONTAGEM DOS PRAZOS**

Na contagem dos prazos estabelecidos neste contrato, excluir-se-á o dia do início e incluir-se-á o do vencimento, e considerar-se-ão os dias consecutivos, exceto quando for explicitamente disposto em contrário, conforme art. 110 da Lei n.º 8.666/1993.



### **CLÁUSULA DÉCIMA NONA – DO FORO DE ELEIÇÃO**

Fica eleito o Foro da Justiça Federal, Seção Judiciária do Rio de Janeiro, para dirimir qualquer litígio decorrente do presente contrato que não possa ser resolvido por meio consensual e amigável, com expressa renúncia a qualquer outro, por mais privilegiado que seja.

E, por estarem assim acordes em todas as condições e cláusulas estabelecidas neste contrato, firmam as partes o presente instrumento em 03 (três) vias de igual teor e forma e para um mesmo efeito, depois de lido e achado conforme, em presença de testemunhas abaixo firmadas.

Rio de Janeiro, [data]

### **CONSELHO REGIONAL DE ENFERMAGEM DO RIO DE JANEIRO – COREN-RJ**

#### **EMPRESA CONTRATADA**

#### **TESTEMUNHAS:**

1<sup>a</sup> \_\_\_\_\_

2<sup>a</sup> \_\_\_\_\_

NOME:

NOME:

CPF:

CPF