EDITAL
PREGÃO ELETRÔNICO Nº 008/2020 - UASG: 925403
Processo Administrativo nº 2020/568274

1. PREÂMBULO

O Instituto de Gestão Previdenciária do Estado do Pará – IGEPREV, CNPJ: 05.873.910/0001-00. Autarquia dotada de personalidade jurídica de direito público, com sede e foro em Belém, Capital do Estado do Pará, neste ato representado por seu Presidente, Sr. ILTON GIUSSEPP STIVAL MENDES DA ROCHA LOPES DA SILVA, tendo sido designado o Pregoeiro e a Equipe de Apoio pela Portaria nº 231, de 08 de julho de 2020, publicada no Diário Oficial do Estado nº 34.276 de 09 de julho de 2020, levam ao conhecimento dos interessados que realizará licitação na modalidade PREGÃO **ELETRÔNICO**, do tipo **MENOR PREÇO**, tendo por critério de julgamento o valor do **GLOBAL**, modo de disputa **ABERTO E FECHADO**, sob o regime de execução indireta, nas condições estabelecidas neste Edital e seus Anexos. O procedimento licitatório obedecerá ao disposto seguinte legislação**: Lei nº 10.520**, de 17 de julho de 2002 (Institui, no âmbito da União, Estados, Distrito Federal e Municípios, modalidade de licitação denominada pregão); **Decreto Federal nº 10.024**, de 20 de setembro de 2019(Regulamenta o pregão na forma eletrônica); **Lei Estadual n° 6.474**, de 06 de agosto de 2002; **Decreto Estadual nº 534**, de 4 de fevereiro de 2020; **Lei Complementar Federal nº 123**, de 14 de dezembro de 2006 (Estatuto da microempresa e empresa de pequeno porte) e sua alteração LC 147/14; **Decreto Estadual nº 878**, de 31 de março de 2008 (Regulamenta o tratamento diferenciado e simplificado para microempresa e empresa de pequeno porte no âmbito da Administração Pública Estadual); **Decreto Estadual nº 877**, de 31 de março de 2008 (Dispõe sobre o pagamento de fornecedores da Administração Pública e Indireta do Governo do Estado do Pará); subsidiária a **Lei Federal n° 8.666**, de 21 de junho de 1993 (Lei de licitações e contratos administrativos) e legislação correlata, bem como, as exigências previstas neste Edital e seus anexos.

2. INFORMAÇÕES GERAIS

A licitação será realizada em sessão pública, por meio da Internet, mediante condições de segurança – criptografia e autenticação – em todas as suas fases. A retirada do edital se dará a partir da data de publicação do aviso no Diário Oficial do Estado, nos sites de compras do Governo Federal www.comprasgovernamentais.gov.br e do Governo Estadual www.compraspara.pa.gov.br.

-Data da Realização: **12/11/2020**

-Horário: 10:00h (Horário de Brasília)

- Acesso eletrônico à participação: www.comprasgovernamentais.gov.br

-Acesso ao edital: **www.compraspara.pa.gov.br ou www.comprasgovernamentais.gov.br, www.igeprev.pa.gov.br**

-UASG: 925403 – Instituto de Gestão Previdenciária do Estado do Pará.

2.1 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e endereço eletrônico estabelecidos no item acima, desde que não haja comunicação da Pregoeira em contrário.

2.2. **Os pedidos de esclarecimentos** e informações referentes ao processo licitatório deverão ser enviados à Pregoeira, até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, **exclusivamente** por meio eletrônico via internet, através do e-mail: **licitacoes@igeprev.pa.gov.br,** devendo o Licitante mencionar o número do processo licitatório.

2.2.1 O pregoeiro responderá aos pedidos de esclarecimentos no prazo de (2) dois dias úteis, contado da data de recebimento do pedido, e poderá requisitar subsídios formais aos responsáveis pela elaboração do edital e dos anexos.

2.2.2 As respostas aos pedidos de esclarecimentos serão divulgadas pelo sistema e vincularão os participantes e a administração

2.3 **As impugnações** a este edital poderão ser feitas, por qualquer pessoa, até 02 (dois) dias úteis antes da data fixada para abertura da Sessão Pública, na forma eletrônica via internet, através do e-mail: **licitacoes@igeprev.pa.gov.br**, decaindo desse direito quem não o fizer no prazo estipulado. Apontando as falhas ou irregularidades que o viciariam.

2.3.1 A impugnação não possui efeito suspensivo e caberá ao pregoeiro, auxiliado pelos responsáveis pela elaboração do edital e dos anexos, decidir sobre a impugnação no prazo de 24 (vinte e quatro) horas, contado da data de recebimento da impugnação.

2.3.2 A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo pregoeiro, nos autos do processo de licitação.

2.3.2 Acolhida a impugnação contra o edital, será definida e publicada nova data para realização

do certame.

3. DO OBJETO

3.1 Contratação de Empresa Especializa na Prestação de Serviços de Atividade de Execução Continuada à prestação de Serviço Gerenciados de Segurança Lógica através de uma Solução Integrada composta por serviços complementares como suporte técnico e monitoração preventiva, dentre outros, e a alocação de hardware(s) e/ou software(s) necessários para a execução do serviço.

3.2 Em caso de discordância existente entre as especificações do objeto descritas no Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

3.3 Maiores detalhes sobre a execução do serviço, bem como informações complementares para melhor dimensionamento da proposta, constam em Termo de Referência, anexo a este Edital.

4. DO CREDENCIAMENTO

4.1. O Credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico, no site http://www.comprasgovernamentais.gov.br.

4.2. O Credenciamento do licitante dependerá de registro cadastral atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF, que também será requisito obrigatório para fins de habilitação.

4.3. O Credenciamento junto ao provedor do sistema implica a responsabilidade legal do licitante, ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao Pregão Eletrônico.

4.4. O uso da senha de acesso pelo licitante é de sua responsabilidade exclusiva, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao IGEPREV, promotor da licitação, responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros.

5. DA DOTAÇÃO ORÇAMENTÁRIA E FINANCEIRA

5.1. As despesas decorrentes desta licitação correrão por conta da classificação orçamentária:

5.1.1. Unidade Orçamentária: 84201 – IGEPREV;

- Unidade Orçamentária: 84201- Instituto de Gestão Previdenciária do Estado do Pará;
- Unidade Gestora: 840201 - Instituto de Gestão Previdenciária do Estado do Pará;
- Programa do PPA 2020/2023: 1508 – Governança Pública;
- Classificação Funcional Programática: 09.126.1508-8238: Gestão de Tecnologia da Informação e Comunicação;
- Fonte de Recursos: 0261000000: Recursos Diretamente Arrecadados pela Administração Indireta;
- Nº DA AÇÃO: 246021;
- Natureza de Despesa: 339040 – Serviços de Tec. da Informação e Comunicação - PJ

6. DA PARTICIPAÇÃO NA LICITAÇÃO

6.1. Caberá ao licitante interessado em participar do pregão, na forma eletrônica:

I Credenciar-se previamente no Sicaf ou, na hipótese de que trata o §2º do art. 5º, no sistema eletrônico utilizado no certame;

II Remeter, no prazo estabelecido, exclusivamente via sistema, os **documentos de habilitação e a proposta** e, quando necessário, os documentos complementares;

III Responsabilizar-se formalmente pelas transações efetuadas em seu nome, assumir como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros;

IV Acompanhar as operações no sistema eletrônico durante o processo licitatório e responsabilizar-se pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pelo sistema ou de sua desconexão.

6.2. Como requisito para a participação neste Pregão a licitante deverá manifestar, em campo

próprio do Sistema Eletrônico, que detém a condição de microempresa (ME) ou empresa de pequeno porte (EPP), nos termos da Lei Complementar nº. 123 de 14 de dezembro de 2006, assim como manifestar-se em campo próprio do sistema, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências previstas neste instrumento convocatório, declarar a inexistência de fato superveniente impeditivo de sua habilitação e que não emprega menores de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre ou menor de dezesseis anos, em qualquer trabalho, salvo na condição de aprendiz, a partir de quatorze anos.

6.3 As declarações mencionadas acima deverão ser enviadas de forma virtual, ou seja, o fornecedor no momento da elaboração e envio de proposta, também enviará as referidas declarações pelo sistema, as quais serão baixadas (download) pelo pregoeiro na fase de habilitação e inclusas no respectivo processo.

6.4 A declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

6.5 **Não poderão participar deste Pregão Eletrônico**:

6.5.1 Empresas declaradas inidôneas para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade;

6.5.2 Cooperativas.

6.5.3 Quaisquer interessados que se enquadrem nas vedações previstas no artigo 9º da Lei n.º 8.666/93.

6.6 O descumprimento de qualquer condição de participação ou a declaração falsa relativa ao cumprimento de qualquer condição sujeitará o licitante às sanções previstas em lei e neste Edital.

6.7 Será admitida a subcontratação para serviços complementares.

7 DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

7.1 A licitante deverá elaborar sua proposta considerando o **VALOR GLOBAL PARA OS 36 (TRINTA E SEIS) MESES DE CONTRATO**.

7.2 Os licitantes encaminharão, exclusivamente por meio do sistema, concomitantemente com os documentos de habilitação exigidos no edital, proposta com a descrição do objeto ofertado e o preço, até a data e o horário estabelecidos para abertura da sessão pública, quando, então, encerrar-se-á automaticamente a etapa de envio dessa documentação.

7.3 O envio da proposta, acompanhada dos documentos de habilitação exigidos neste Edital, ocorrerá por meio de chave de acesso e senha.

7.4 As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123, de 2006.

7.5 Até a abertura da sessão pública, os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema;

7.6 Não será estabelecida, nessa etapa do certame, ordem de classificação entre as propostas apresentadas, o que somente ocorrerá após a realização dos procedimentos de negociação e julgamento da proposta.

7.7 Os documentos que compõem a proposta e a habilitação do licitante melhor classificado somente serão disponibilizados para avaliação do pregoeiro e para acesso público após o encerramento do envio de lances.

7.8 Os documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos no edital e já apresentados, serão encaminhados pelo licitante melhor classificado após o encerramento do envio de lances, no prazo de 2 (duas) horas, conforme § 2º do art. 38 do Decreto Estadual nº 534/2020.

7.9 O licitante declarará, em campo próprio do sistema, o cumprimento dos requisitos para a habilitação e a conformidade de sua proposta com as exigências do edital.

7.10 A falsidade da declaração de que trata o subitem 7.9 sujeitará o licitante às sanções previstas em lei.

8 DO PREENCHIMENTO DA PROPOSTA

8.1 A licitante deverá consignar, na forma expressa no sistema eletrônico, o preço, a descrição minuciosa do objeto ofertado, devendo constar procedência e todos os detalhes de

relevância do objeto, já considerados e inclusos todos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto.

8.2 As propostas terão validade de, no mínimo, 60 (sessenta) dias.

8.3 Serão desclassificadas:

a. As propostas que não atendam às exigências ao ato convocatório da licitação;

b. As propostas que apresentarem valores unitários e/ou global, manifestamente inexequíveis, assim considerados aqueles que não venham a ter demonstrado sua viabilidade através de documentação que comprove que os custos dos insumos são coerentes com os de mercado e que os coeficientes de produtividade são compatíveis com a execução do objeto do contrato, bem como aqueles que não atenderem ao § 3º, art. 44 da Lei n.º 8.666/93;

8.4 A inclusão na proposta de item de custo vedado não acarretará a desclassificação do licitante, devendo o pregoeiro determinar que os respectivos custos sejam excluídos da Planilha, adotando, se for o caso, as providências do art. 26, § 3º, do Decreto n.º 5.450/05.

8.5 Na hipótese de contratação com a previsão de itens de custos vedados, tais valores serão glosados e os itens serão excluídos da Planilha, garantidas ampla defesa e contraditório.

9. DA ABERTURA DA SESSÃO PÚBLICA

9.1. A abertura da sessão pública deste **Pregão**, conduzida pelo **Pregoeiro**, ocorrerá na data e na hora indicadas no preâmbulo deste Edital, no sítio www.comprasgovernamentais.gov.br.

9.2. Durante a sessão pública, a comunicação entre o **Pregoeiro** e as **licitantes** ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

9.3. Cabe à **licitante** acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

10. DA CONFORMIDADE DAS PROPOSTAS

10.1. O pregoeiro verificará as propostas apresentadas e desclassificará aquelas que não estejam em conformidade com os requisitos estabelecidos no edital.

10.2. A desclassificação da proposta será fundamentada e registrada no sistema, acompanhado em tempo real por todos os participantes.

10.3. O sistema ordenará automaticamente as propostas classificadas pelo pregoeiro.

10.4. Classificadas as propostas, o pregoeiro dará início à fase competitiva, oportunidade em que os licitantes poderão encaminhar lances exclusivamente por meio do sistema eletrônico.

10.5. Somente as **licitantes** com propostas classificadas participarão da fase de envio de lances.

11. DA FORMULAÇÃO DE LANCES

11.1. Aberta a etapa competitiva, as **licitantes** poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo imediatamente informadas do horário e valor consignados no registro de cada lance.

11.2. Não serão aceitos dois ou mais lances iguais e prevalecerá aquele que for recebido e registrado primeiro.

11.3. Durante a sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

11.4. Os lances apresentados e levados em consideração para efeito de julgamento de aceitação/classificação da proposta serão de exclusiva e total responsabilidade da **licitante**, não lhe cabendo o direito de pleitear qualquer alteração.

11.5. Durante a fase de lances, o **Pregoeiro** poderá excluir, justificadamente, lance cujo valor seja manifestamente inexequível.

11.6. Se ocorrer a desconexão para o **Pregoeiro** no decorrer da etapa de lances, e o sistema eletrônico permanecer acessível às **licitantes,** os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

11.7. No caso de a desconexão para a **Pregoeira** persistir por tempo superior a 10 (dez) minutos, a sessão do **Pregão** será suspensa e terá reinício somente após comunicação expressa às participantes no sítio www.comprasgovernamentais.gov.br.

11.8. Após a etapa de envio de lances, haverá a aplicação dos critérios de desempate previstos nos art. 44 e art. 45 da Lei Complementar nº 123, de 14 de dezembro de 2006, seguido da aplicação do critério estabelecido no § 2º do art. 3º da Lei nº 8.666, de 1993, se não houver licitante que atenda à primeira hipótese.

11.9. Os critérios de desempate serão aplicados nos termos do subitem 11.8, caso não haja envio de lances após o início da fase competitiva.

11.10. Na hipótese de persistir o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

12. DA NEGOCIAÇÃO E DA ACEITABILIDADE DA PROPOSTA

12.1. Após o encerramento da etapa de lances, o Pregoeiro deverá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao licitante que tenha apresentado o lance mais vantajoso, para que seja obtida melhor proposta, observado o critério de julgamento e o valor estimado para a contratação, não se admitindo negociar condições diferentes das previstas neste Edital. (art. 38 do Decreto Estadual n.º 534/2020).

12.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

12.3. Encerrada a negociação a licitante detentora da melhor oferta deverá enviar sua Proposta de Preços assinada, digitalizada e **atualizada** em conformidade com o último lance ofertado **no prazo de 02 (duas) horas**, contado da convocação efetuada pela **Pregoeira** por meio da opção "Enviar Anexo" no sistema Comprasnet.

12.4. O valor da Proposta deverá englobar todas as despesas referentes ao fornecimento, bem como todos os tributos, frete até o destino (sede da IGEPREV), encargos sociais e trabalhistas e quaisquer outras despesas e insumos que incidam ou venham a incidir sobre o objeto desta licitação.

12.5. A omissão de qualquer despesa necessária à perfeita execução do objeto desta licitação, inclusive quanto à entrega e/ou descarga, será interpretada como não existente ou já incluída no preço, não podendo a licitante pleitear acréscimos após a aceitação da proposta.

12.6. Na formulação da Proposta de Preços, o licitante deve informar os seguintes dados:

a. Preço ajustados ao lance final, **anual, unitário e total**, em valor líquido em moeda corrente nacional, com aproximação de até duas casas decimais, não podendo exceder o valor do lance final.

b. Informar a marca do produto a ser entregue, se for o caso.

c. Informar o nome do Banco, número da Agência e número da Conta Corrente para efeito de depósito referente ao pagamento, na forma do Decreto Estadual n.º 877, de 31 de março de

2008, publicado no DOE n.º 31.139, de 01/04/2008 e Instrução Normativa n.º 0018, de 21 de maio de 2008 da Secretaria de Estado da Fazenda – SEFA, publicada no DOE n.º 31.174, de 23/05/2008.

c.1 Caso a licitante não possua, desde já, conta corrente no Banco do Estado do Pará S/A – BANPARÁ, se compromete, por ocasião da contratação, em providenciar a abertura de conta corrente para receber os pagamentos decorrentes da contratação deste pregão.

d. O prazo de validade de Proposta de Preços apresentada é de 60 (sessenta) dias a contar da data de seu recebimento (art. 9º, inciso XXVIII da Lei Estadual n.º 6.474/2002, combinado com o art. 28, § 4º do Decreto Estadual n.º 2.069/2006).

12.7. Se a oferta não for aceitável ou se o proponente não atender às exigências editalícias, o Pregoeiro examinará as ofertas subsequentes, na ordem de classificação, até a apuração de uma proposta que atenda todas as exigências.

12.8. Após a apresentação da proposta, não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pelo pregoeiro.

12.9. Decorrido o prazo de validade das propostas, sem convocação para contratação, fica a licitante vencedora liberadas dos compromissos assumidos.

13. DA HABILITAÇÃO

13.1. A habilitação da licitante vencedora será verificada "on-line" no Sistema de Cadastramento Unificado de Fornecedores – SICAF, no sítio www.tst.jus.br/certidao a Certidão Negativa de Débitos Trabalhistas, após a análise e julgamento da Proposta, devendo ainda incluir:

13.1.1. A LICITANTE deve possuir atestado(s) de capacidade técnica, focado(s) em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde são ou foram prestados pelo menos os seguintes serviços que compõem o objeto deste Edital: Firewall Próxima Geração e VPN, Proteção das Estações de Trabalho e Servidores de Rede e Gestão de Credenciais Privilegiadas, conferido por empresas públicas ou privadas. O(s) atestado(s) deve(m) comprovar que a(s) rede(s) gerenciada(s) somam, pelo menos, 500 (quinhentos) hosts;

13.1.2. Certidão negativa de falência ou concordata, expedida pelo cartório distribuidor da sede da licitante ou certidão negativa de execução patrimonial, expedida pelo cartório distribuidor do domicílio da pessoa física (proprietária ou sócia da empresa licitante), dentro do prazo de validade estabelecido pelo emitente da certidão. (Inciso II do art.31 da Lei 8.666/93), e data de emissão não

superior a 90 (noventa) dias.

13.1.3. Comprovação da boa situação financeira da licitante, aferida com base nos índices de liquidez geral (LG), solvência geral (SG) e liquidez corrente (LC) maiores que um (>1), analisadas e informadas automaticamente pelo SICAF, conforme item 7-V da IN/MARE nº 05/95.

13.2. Os documentos necessários à habilitação poderão ser apresentados em original, ou em cópia autenticada em cartório competente ou publicação em órgão da imprensa oficial ou em cópias simples acompanhadas do original para cotejamento.

13.3. Não serão aceitos "protocolos de entrega" ou "solicitação de documento" em substituição aos documentos requeridos no presente Edital e seus Anexos;

13.4. Serão inabilitadas as empresas que não atenderem as exigências deste item 13 do Edital.

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

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

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

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

14 DO RECURSO

14.1 Declarado o vencedor, o **Pregoeiro** abrirá prazo de mínimo 30 (trinta) minutos, durante o qual qualquer **licitante** poderá, de forma imediata e motivada, em campo próprio do sistema, manifestar sua intenção de recurso.

14.2 A **licitante** que tiver sua intenção de recurso aceita deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 3 (três) dias, ficando as demais **licitantes**, desde logo,

intimadas a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente.

14.3 O **Pregoeiro** examinará a intenção de recurso, aceitando-a ou, motivadamente, rejeitando-a, em campo próprio do sistema.

14.4 A ausência de manifestação no prazo estabelecido autoriza o **Pregoeiro** a adjudicar o objeto à **licitante vencedora**.

14.5 Para efeito do disposto no § 5º do artigo 109 da Lei nº 8.666/1993, fica a vista dos autos do processo franqueada aos interessados.

14.6 À autoridade competente cabe decidir os recursos contra os atos do Pregoeiro, quando este mantiver sua decisão (art. 45 do Decreto Estadual n.º 534/2020).

14.7 O acolhimento do recurso implicará a invalidação apenas dos atos insuscetíveis de aproveitamento.

15 DA REABERTURA DA SESSÃO PÚBLICA

15.1 A sessão pública poderá ser reaberta:

15.1.1 Nas hipóteses de provimento de recurso que leve à anulação de atos anteriores à realização da sessão pública precedente ou em que seja anulada a própria sessão pública, situação em que serão repetidos os atos anulados e os que dele dependam.

15.1.2 Quando houver erro na aceitação do preço melhor classificado ou quando o licitante declarado vencedor não assinar o contrato, não retirar o instrumento equivalente ou não comprovar a regularização fiscal e trabalhista, nos termos do art. 43, §1º da LC nº 123/2006. Nessas hipóteses, serão adotados os procedimentos imediatamente posteriores ao encerramento da etapa de lances.

15.2 Todos os licitantes remanescentes deverão ser convocados para acompanhar a sessão reaberta.

15.3 A convocação se dará por meio do sistema eletrônico (“chat”), e-mail, ou, ainda, e-mails, de acordo com a fase do procedimento licitatório.

15.4 A convocação feita por e-mail dar-se-á de acordo com os dados contidos no SICAF, sendo responsabilidade do licitante manter seus dados cadastrais atualizados.

16 DA ADJUDICAÇÃO E HOMOLOGAÇÃO

16.1 O objeto deste Pregão será adjudicado pelo Pregoeiro, salvo quando houver recurso, hipótese em que a adjudicação caberá à autoridade competente para homologação.

16.2 A homologação deste Pregão compete ao Presidente do Instituto de Gestão Previdenciária do Estado do Pará - IGEPREV.

17 DO SANEAMENTO DA PROPOSTA E DA HABILITAÇÃO

17.1 O pregoeiro poderá, no julgamento da habilitação e das propostas, sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível aos licitantes, e lhes atribuirá validade e eficácia para fins de habilitação e classificação, observado o disposto na Lei nº 8.972, de 13 de janeiro de 2020.

17.2 Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o caput, a sessão pública somente poderá ser reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, e a ocorrência será registrada em ata.

18 DO INSTRUMENTO CONTRATUAL

18.1 Após a homologação, o adjudicatário será convocado para assinar o contrato no prazo de 10 (dez) dias.

18.2 Na assinatura do contrato, será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato.

18.3 Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato, outro licitante poderá ser convocado, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato, sem prejuízo da aplicação das sanções de que trata o art. 49.

18.4 O prazo de validade das propostas será de 60 (sessenta) dias.

19 DAS SANÇÕES ADMINISTRATIVAS

19.1 Pela inexecução total ou parcial do objeto deste Pregão, o Instituto poderá garantida a prévia defesa, aplicar à licitante vencedora as seguintes sanções:

19.1.1 Advertência, que será aplicada através de notificação por meio de ofício, mediante contrarrecibo do representante legal da empresa, no caso de pequenas falhas e/ou irregularidades, estabelecendo o prazo de 05 (cinco) dias úteis para que a empresa licitante apresente justificativas, que só serão aceitas mediante crivo da Administração;

19.1.2 Multa no atraso injustificado na entrega do objeto licitado ao **CONTRATANTE** após a data preestabelecida, quando do envio dos dados, e/ou as obrigações parciais estabelecidas neste edital, sujeitará ao **CONTRATADO** a multa, na forma estabelecida a seguir:

19.1.2.1 Até 30 (trinta) dias, após o prazo citado acima, multa de 0,3% (zero vírgula três por cento) ao dia;

19.1.2.2 Após os 30 (trinta) dias citados no item 19.1.2.1 multa de 0,5% (zero vírgula cinco por cento) ao dia; configurando-se após esse prazo a inexecução do contrato;

19.1.2.3 As multas a que se referem os subitens acima incidem sobre o valor global do produto que deveria ser entregue e será deduzido no pagamento da Nota Fiscal, sem embargo de indenização dos prejuízos porventura causados ao Instituto.

19.2 Ficará impedida de licitar com a Instituição, pelo prazo de até 05 (cinco) anos, garantindo o direito prévio da citação e de ampla defesa, enquanto perdurar os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, a licitante que:

19.2.1 não assinar o contrato ou a ata de registro de preços;

19.2.2 não entregar a documentação exigida no edital;

19.2.3 apresentar documentação falsa;

19.2.4 causar o atraso na execução do objeto;

19.2.5 não mantiver a proposta;

19.2.6 falhar na execução do contrato;

19.2.7 fraudar a execução do contrato;

19.2.8 comportar-se de modo inidôneo;

19.2.9 declarar informações falsas; e

19.2.10 cometer fraude fiscal.

19.3 As sanções de advertência e de impedimento de licitar e contratar com a Instituição serão aplicados à licitante vencedora juntamente com a de multa, descontando-a dos pagamentos a serem efetuados, facultada a defesa prévia do interessado, no respectivo processo, no prazo de até 05 (cinco) dias úteis.

19.4 O atraso injustificado na execução, conforme estipulado no Edital, por período superior a 30 (trinta) dias, poderá ensejar a desclassificação da referida empresa.

19.5 As sanções serão registradas e publicadas no Sicaf e no Sistema Integrado de Materiais e Serviços (SIMAS).

20 DO PAGAMENTO

20.1 A **CONTRATADA** apresentará nota fiscal eletrônica para liquidação e pagamento da despesa pela **CONTRATANTE**, através de ordem bancária creditada em conta corrente no Banco do Estado do Pará – BANPARÁ S/A, conforme Decreto Estadual nº 877/2008, no prazo de 30 (trinta) dias, contados da apresentação da nota fiscal devidamente atestada pelo servidor designado.

20.2 No caso de devolução da nota fiscal, o prazo de pagamento estipulado no subitem anterior passará a ser contado a partir da data de reapresentação dos referidos documentos.

20.3 A **CONTRATANTE** poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela **CONTRATADA**, nos termos deste Contrato.

20.4 A **CONTRATANTE** poderá, ainda, deduzir do montante a ser pago(s) valor(es) correspondente(s) às interrupções, atrasos ou não prestação de serviço, conforme dispõe o presente Contrato.

20.5 O atraso no pagamento acarretará multa moratória diária de 0,33 (zero vírgula trinta e três por cento) por dia, sobre o valor da parcela atrasada, limitado a 10% (dez por cento) do valor

do contrato, mediante provocação da **CONTRATADA**, e mediante aprovação do Ordenador de Despesa da **CONTRATANTE**.

20.6 A **CONTRATANTE** efetuará os pagamentos mediante Ordem Bancária e para tanto, a **CONTRATADA** deverá informar no documento de cobrança, o nome e o número do banco, a agencia e conta corrente onde será creditado o pagamento. A Conta Corrente somente deverá estar em nome da **CONTRATADA**, de acordo com o Decreto Estadual n° 877, de 31 de março de 2008.

20.7 Parcela fixa mensal pela prestação dos serviços de manutenção e suporte técnico da solução, a ser paga até o décimo dia do mês subsequente da prestação do serviço, estando o pagamento da primeira parcela condicionada após passado o primeiro mês da assinatura do contrato.

20.8 Nenhum pagamento será efetivado sem que representantes do IGEPREV atestem, por meio de Termo de Aceite e/ou Termo de Homologação, que o objeto contratado está integralmente sendo entregue/disponibilizado e/ou cumprido pela CONTRATADA.

20.9 Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência contratual.

20.10 Sem prejuízo ao pagamento das multas estipuladas no contrato, o IGEPREV poderá suspender quaisquer pagamentos devidos à CONTRATADA, sem incorrer em ônus adicionais, sempre que sua área gestora do contrato constatar a ocorrência de atrasos na execução do objeto contratado, retomando-os tão logo tais atrasos sejam completamente eliminados nos termos de parecer da área gestora do contrato.

20.11 Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário, e órgãos administrativos, atribuídos ao IGEPREV, oriunda de problemas na execução do contrato por parte da CONTRATADA, serão repassadas a esta e deduzidas do pagamento realizado pelo IGEPREV, independente de comunicação ou interpelação judicial ou extrajudicial.

20.12 No preço apresentado pela CONTRATADA já estão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o contrato, assim como contribuições previdenciárias, fiscais e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho, e outros, ficando excluída qualquer solidariedade do IGEPREV, por eventuais autuações.

20.13 A realização de qualquer pagamento pelo IGEPREV fica condicionada a apresentação dos seguintes documentos: CND- emitida pelo INSS, Certidão de Regularidade da Receita Federal e da PGFN, CND do FGTS expedida pela CEF; prova de regularidade para com as fazendas Estadual e Municipal do domicílio da sede da CONTRATADA.

20.14 Será procedida consulta "ON LINE" junto ao SICAF antes de cada pagamento a ser efetuado ao fornecedor, para verificação da situação do mesmo, relativamente às condições exigidas no empenho, cujos resultados serão impressos e juntados aos autos do processo próprio.

20.15 Constatada a irregularidade fiscal e/ou trabalhista, a **CONTRATANTE** poderá aplicar, garantido o contraditório e a ampla defesa, as penalidades decorrentes do art. 87 da lei 8.666/93.

21 DA ANULAÇÃO E REVOGAÇÃO

21.1 A autoridade competente para homologar este certame poderá revogar a licitação em face de razões de Interesse Público, derivadas de fato superveniente devidamente comprovado, pertinente e suficiente para justificar tal conduta, devendo anulá-la por ilegalidade, de ofício ou por provocação de qualquer pessoa, mediante ato escrito e fundamentado.

21.2 A anulação do procedimento licitatório induz ao do contrato.

21.3 Os licitantes não terão direito a indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do fornecedor de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do contrato condições deste Edital.

21.4 No caso de desfazimento de processo licitatório, fica assegurado o direito ao contraditório e à ampla defesa.

22 DISPOSIÇÕES FINAIS

22.1 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e endereço eletrônico anteriormente estabelecido, desde que não haja comunicação, da pregoeira em contrário.

22.2 Esta licitação poderá ser revogada por interesse da Administração, em decorrência de fato

superveniente devidamente comprovado, pertinente e suficiente para justificar o ato, ou anulada por vício ou ilegalidade, a modo próprio ou por provocação de terceiros, sem que as licitantes tenham direito a qualquer indenização, obedecendo ao disposto no Art. 18, do Decreto n° 3.555/00.

22.3 Qualquer modificação no presente EDITAL será divulgada pela mesma forma que se divulgou o texto original, reabrindo-se o prazo inicialmente estabelecido, exceto quando, inquestionavelmente, a alteração não afetar a formulação da proposta (Art. 20, Parágrafo único, do Decreto nº 5.450/05).

22.4 É facultado ao pregoeiro ou à autoridade competente, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou complementar a instrução do processo, vedada a inclusão posterior de documento ou informação que deveria constar originariamente da proposta.

22.5 Os proponentes são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

22.6 Após apresentação da proposta não caberá desistência, salvo por motivo justo decorrente de fato superveniente e aceito pela pregoeira.

22.7 A homologação do resultado desta licitação não implicará direito a realização do serviço pela Administração.

22.8 Na contagem dos prazos estabelecidos neste Edital e seus Anexos excluir-se-á o dia do início e incluir- se-á o do vencimento, vencendo-se os prazos somente em dias de expediente normal.

22.9 O desatendimento de exigências formais não essenciais não importará no afastamento da licitante, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta, durante a realização da sessão pública de Pregão.

22.10 As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre os interessados, sem comprometimento do interesse da Administração, a finalidade e a segurança da contratação.

22.11 É vedada a subcontratação total ou parcial do objeto deste certame.

22.12 O esclarecimento de dúvidas a respeito de condições do edital e de outros assuntos relacionados à presente licitação serão divulgados mediante publicação de notas na página web,

no endereço **www.comprasgovernamentais.gov.br**, opção "Fornecedores/Licitações", ficando as licitantes obrigadas a acessá-la para a obtenção das informações prestadas pela pregoeira.

22.13 Serão verificadas na fase de habilitação a existência de registros impeditivos da contratação no Cadastro Nacional de Empresas Inidôneas e Suspensas, disponível no Portal da Transparência **www.portaltransparencia.gov.br**; a existência de registros impeditivos de contratação por ato de improbidade administrativa disponível no portal do Conselho Nacional de Justiça – CNJ; e a existência de débitos inadimplidos perante a justiça do trabalho disponível no site www.tst.jus.br/certidao, sob pena de inabilitação.

23 DOS ANEXOS

23.1 São partes integrantes deste Edital os seguintes anexos:

a) Anexo I - Termo de Referência;

b) Anexo II – Modelo de proposta;

c) Anexo III – Declaração que emprega 5% de pessoas com deficiência);

d) Anexo IV – declaração de cumprimento das normas trabalhistas, de proteção ao meio ambiente e aos direitos da mulher;

e) Anexo V – Minuta de Contrato; e

23.2 Todas as declarações mencionada são de envio obrigatório, devendo ser anexadas junto com aos documentos de habilitação e proposta em campo próprio do sistema.

24 DO FORO

24.1 O Foro é o da Justiça Estadual, Seção Judiciária de Belém - Pará, para dirimir quaisquer litígios oriundos deste Pregão.

Belém - PA, 29 de outubro de 2020.

Cícero Marcos L. Rosário

Pregoeiro

ANEXO I – TERMO DE REFERÊNCIA

1. OBJETO

Contratação de Empresa Especializa na Prestação de Serviços de Atividade de Execução Continuada à prestação de Serviço Gerenciados de Segurança Lógica através de uma Solução Integrada composta por serviços complementares como suporte técnico e monitoração preventiva, dentre outros, e a alocação de hardware(s) e/ou software(s) necessários para a execução do serviço.

2. DESCRIÇÃO DOS SERVIÇOS

Serviços de Atividade de Execução Continuada refere-se :

- Serviço de Proteção de Perímetro com Firewall Avançado de Próxima Geração, para controle do tráfego nos segmentos protegidos;
- Serviço de Proteção das Estações de Trabalho e Servidores de Rede (Tanto físicos, quanto virtuais) para identificar e mitigar infecções por malwares;
- Serviço de Gestão de Credenciais Privilegiadas;
- Disponibilização de banco de até 4.000 (quatro mil) horas para a prestação de serviços técnicos, que possam ser utilizadas sob demanda.

2.1. IMPLANTAÇÃO DAS SOLUÇÕES

2.1.1. A CONTRATADA deverá implantar as soluções da(s) FABRICANTE(S), que compõem a solução integrada, com configuração, instalação e fornecimento dos hardwares e softwares relacionados, em regime de comodato, para o seguinte escopo:

2.1.1.1. Serviço de Proteção de Perímetro com Firewall Avançado de Próxima Geração;

2.1.1.2. Serviço de Proteção das Estações de Trabalho e Servidores de Rede;

2.1.1.3. Serviço de Gestão de Credenciais Privilegiada;

2.1.2. A Solução Integrada de Serviços Gerenciados de Segurança deverá englobar alocação de equipamentos, produtos, peças, softwares e tudo mais que se fizer necessário à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos equipamentos e softwares utilizados bem como os serviços de monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana);

2.1.3. A CONTRATADA deverá fornecer todos os equipamentos, softwares, licenças e atualizações necessárias para a prestação do serviço, implantar toda a solução, capacitar a equipe

técnica indicada pelo IGEPREV e sobre a solução prestar suporte técnico especializado, compreendendo administração, monitoramento com resposta a incidentes de segurança e suporte técnico 24 (vinte e quatro) horas por

dia, 7 (sete) dias por semana, de acordo com cada serviço do Catálogo de Serviço, durante toda a vigência do contrato.

2.1.4. Todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos do *IGEPREV;*

2.1.5. A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados);

2.1.6. A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do *IGEPREV,* sem prejuízo aos serviços desta;

2.1.7. A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Termo de Referência deverá ser executada pela CONTRATADA no prédio do IGEPREV, localizado na *Av. Alcindo Cacela, 1962, Belém/PA*, sem custos adicionais para o *IGEPREV.*

2.2. PRESTAÇÃO DOS SERVIÇOS CONTÍNUOS

2.2.1. Os serviços específicos de monitoração de incidentes de segurança deverão ser prestados de forma remota a partir de Centros de Operação de Segurança (SOC) próprios, localizados no Brasil, estritamente de acordo com as especificações deste documento;

2.2.1.1. Os serviços de monitoração providos pelos Centros de Operação de Segurança (SOC) se darão de forma remota e deverão ser realizados pela CONTRATADA, na modalidade 24x7 (vinte e quatro horas por dia, sete dias na semana);

2.2.2. Para a manutenção do hardware e software ofertados, bem como para a prestação de suporte aos serviços de monitoração remota, a CONTRATADA deve possuir infraestrutura de suporte técnico, disponível em período integral, ou seja, 24x7 (vinte e quatro horas por dia, sete dias por semana), nos seguintes modelos:

2.2.2.1. Suporte técnico remoto: suporte prestado por meio de Central de Atendimento 0800 ou equivalente à ligação local, web, e-mail e fax, para:

2.2.2.1.1. Esclarecimento de dúvidas relacionadas à prestação dos serviços, políticas e regras implementadas, funcionalidades da solução e incidentes de segurança, sendo este atendimento imediato;
2.2.2.1.2. Atendimento às solicitações de alterações (inclusão e exclusão) de políticas e regras;
2.2.2.1.3. Atendimento às solicitações de log e relatórios;

2.2.2.2. **Suporte técnico local: atendimento *in loco*, prestados por técnicos capacitados para a solução de problemas relacionados aos produtos fornecidos**.

2.2.3. A CONTRATADA deverá realizar obrigatoriamente manutenções preventivas nas dependências do IGEPREV, por duas vezes ao mês durante toda a vigência do contrato, executados sempre por técnicos treinados e certificados nas soluções fornecidas, com o acompanhamento de um representante da instituição.

2.2.3.1. Poderá ser abrangido também a manutenção corretiva neste momento da manutenção preventiva 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. Esses serviços de assistência técnica deverão ser executados sempre que se fizer necessário, seja por solicitação formal do IGEPREV, seja pelo recebimento de alertas provenientes do sistema de monitoramento.

2.2.4. Todos os custos diretos e indiretos para a realização do atendimento presencial, seja assistência técnica ou manutenção preventiva ou corretiva, serão de responsabilidade da CONTRATADA.

2.2.5. A CONTRATADA deverá disponibilizar um sistema de monitoramento interno, com no máximo 2 televisores de 55 Polegadas, integrado com o sistema de 'Gestão de Evento e Incidentes dos SOCs da CONTRATADA, de modo a permitir que os técnicos do IGEPREV possam acompanhar os alarmes de eventos e de correlação dos logs gerados pelos dispositivos de tecnologia fornecidos.

2.2.6. Para todos os serviços, a contratada deverá criar contas de usuários para que a equipe técnica do *IGEPREV* possa acompanhar e compreender as configurações adotadas. As permissões destas contas serão definidas pelo próprio IGEPREV, mediante assinatura de Termo de Responsabilidade assinado pelo gestor da área de segurança.

2.2.7. Deverão ser apresentados pela CONTRATADA, no mínimo, relatórios analíticos mensais (técnicos e executivos) contendo o diagnóstico dos ambientes monitorados, obtido através do cruzamento das informações coletadas pelos hardwares ou softwares. Tais relatórios deverão estar disponíveis para o IGEPREV, a qualquer momento, se solicitado, inclusive podendo ser de outro *template*, devendo ser disponibilizados em até 24 (vinte e quatro) horas após a solicitação;

2.2.8. A CONTRATADA deverá interagir com os analistas e técnicos do IGEPREV para dirimir dúvidas relacionadas ao serviço prestado;

2.2.9. A CONTRATADA deverá disponibilizar 0800 ou um portal WEB para abertura e acompanhamento de chamados e dirimir dúvidas relacionadas a prestação de serviço;

2.2.10. O IGEPREV informará as pessoas autorizadas a abrir e fechar chamados junto a CONTRATADA bem como o meio pelo qual a autorização de fechamento será formalizada.

2.2.11. Os chamados abertos somente poderão ser fechados após autorização de funcionário designado pelo IGEPREV;

2.3. MANUTENÇÃO DAS REGRAS, POLÍTICAS E VERSÕES DOS SOFTWARES

2.3.1. Toda e qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de "*patches*", etc.) deverão ocorrer mediante autorização do IGEPREV;

2.3.2. As alterações das configurações deverão ocorrer em datas e horários pré- determinados pelo IGEPREV;

2.3.3. O tempo de atendimento das solicitações de alterações das políticas e regras feitas pelo IGEPREV não deverá ultrapassar o SLA (acordo de nível de serviço) especificado neste documento, a contar da efetivação da solicitação;

2.3.4. A CONTRATADA deverá efetuar, em laboratório próprio, os testes necessários antes de implementar qualquer alteração no ambiente de monitoração (políticas, regras, versões, etc.), evitando impactos negativos aos serviços do IGEPREV;

2.3.5. O IGEPREV poderá solicitar, por escrito, o acesso às senhas de configuração dos equipamentos disponibilizados pela CONTRATADA em regime de comodato. O IGEPREV designará duas pessoas para terem acesso a(s) senha(s), que devem ser fornecidas de forma segura. O IGEPREV deverá seguir os procedimentos documentais acordados entre as partes, caso venha a fazer uso deste acesso, e se responsabilizará pelas consequências que por ventura possam advir desteacesso;

2.4. CONTROLE DOS SERVIÇOS REALIZADOS PELA CONTRATADA

2.4.1. Para o controle e administração dos serviços realizados pela CONTRATADA, o IGEPREV poderá nomear até 2 representantes autorizados a interagir com a CONTRATADA. Tais representantes serão responsáveis por:

2.4.1.1. Manter as informações técnicas (configuração do ambiente) atualizadas, bem como dar suporte na implantação e manutenção da solução;
2.4.1.2. Definir as estratégias, políticas e regras a serem implantadas, e analisar os relatórios gerados pelos softwares que compõem a solução;

2.4.1.3. Tomar providências necessárias em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência).

2.4.2. Para cada solução implantada a CONTRATADA emitirá relatórios definidos pelo IGEPREV;

2.4.3. A CONTRATADA realizará reuniões mensais, nas dependências do IGEPREV, para dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos e revisão das configurações e procedimentos implementados;

2.4.4. O IGEPREV poderá realizar auditoria nas instalações do Centro de Operações de Segurança (SOC), com o objetivo de verificar as instalações e a segurança física e

lógica do ambiente e demais itens exigidos neste documento, desde que previamente acordada com a CONTRATADA;

2.5. ARMAZENAMENTO DOS LOGS DE AUDITORIA:

2.5.1. O IGEPREV, caso julgue insuficiente as informações gravadas nos arquivos de logs, poderá solicitar alterações na configuração junto à CONTRATADA;

2.5.2. O tempo de retenção dos logs gerados deverá ser equivalente ao prazo da vigência contratual. Ao final do contrato, a CONTRATADA não deverá ficar com nenhuma cópia dos mesmos, repassando-os para o IGEPREV em meio magnético antes da sua destruição;

2.6. OCORRÊNCIA DE INCIDENTES

2.6.1. No caso de detecção de algum incidente de segurança ou comportamento atípico no ambiente, a CONTRATADA poderá acionar o IGEPREV imediatamente para que sejam tomadas as medidas corretivas e legais necessárias, de acordo com o procedimento de resposta a incidentes;

2.6.2. Serão considerados incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, indisponibilidade dos serviços (DoS), ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade dos serviços do IGEPREV;

2.6.3. A CONTRATADA deverá comunicar imediatamente ao IGEPREV para que possam ser tomadas ações preventivas nos casos de tentativas de: acessos indevidos, de instalação de códigos maliciosos ou de qualquer outra ação que venham pôr em risco a segurança do ambiente do IGEPREV mesmo que a pessoa não obtenha sucesso na tentativa de invasão;

2.6.4. A CONTRATADA deverá disponibilizar todas as informações necessárias (origem do ataque, tipo de ataque, data e hora, logs, etc.) para que sejam apurados os incidentes de segurança reportados;

2.6.5. Dependendo do grau do incidente, a CONTRATADA DEVERÁ enviar recurso técnico capaz de dar suporte ao problema, para compor o tempo de resposta do IGEPREV, visando dirimir quaisquer dúvidas e dar suporte nas providências a serem tomadas.

2.7. SOLUÇÃO DE HARDWARE E SOFTWARE DA CONTRATADA

2.7.1. Os software e hardware necessários para implantação do serviço de monitoração, gerência e administração remota da segurança fazem parte dos serviços a serem prestados pela CONTRATADA durante o prazo do contrato;

2.7.2. A manutenção das licenças do hardware e software necessários, junto aos fabricantes, será de responsabilidade da CONTRATADA, devendo as mesmas estar em nome do IGEPREV, devendo A CONTRATADA apresentar cópia autenticada das mesmas anualmente a CONTRATANTE;

2.7.3. O hardware e software ofertados deverão ser compatíveis com o ambiente operacional do IGEPREV;

2.7.4. A CONTRATADA é responsável pela manutenção preventiva e corretiva do hardware por ela ofertado;

2.7.5. O hardware e o software devem ser fornecidos em regime de comodato.

2.8. ENCERRAMENTO DOS SERVIÇOS DE MONITORAÇÃO REMOTA DA SEGURANÇA

2.8.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a CONTRATADA deverá retirar os componentes da solução, comunicando a retirada ao IGEPREV, por escrito, com 60 dias de antecedência;

2.8.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para o IGEPREV, em mídia magnética ou via rede, e em seguida eliminadas da base de dados da CONTRATADA;

2.8.3. Ao final do contrato a CONTRATADA deverá dar suporte durante toda a fase de transição dos serviços à uma nova CONTRATADA se for o caso.

3. DAS CONDIÇÕES PARA A PRESTAÇÃO DO SERVIÇO.

3.1. Os Centros de Operações de Segurança (SOC) já devem estar em pleno funcionamento na data da abertura deste edital e devem possuir alta disponibilidade, atendendo aos seguintes requisitos:

3.1.1. Os ativos de TI empregados no monitoramento (servidores, rede, software, etc.) deverão estar hospedados em ambiente com as seguintes características mínimas:

3.1.1.1. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia;

3.1.1.2. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por, no mínimo, o prazo do CONTRATO. Após este período deverão ser disponibilizadas para o IGEPREV, em mídia digital ou via rede, e em seguida eliminadas da base de dados da CONTRATADA;

3.1.1.3. Estar configurados de forma que a falha de nenhum dos equipamentos isoladamente interrompa o funcionamento dos sistemas;

3.1.1.4. Estar hospedado em *Datacenter* que deve atender as seguintes especificações:

3.1.1.4.1. Possuir sistemas redundantes para armazenamento de dados e alimentação de energia;

3.1.1.4.2. Possuir estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratados por no mínimo 180 dias. Após este período deverão ser disponibilizadas para o

contratante, em mídia digital ou via rede, e em seguida eliminadas da base de dados da CONTRATADA;

3.1.1.4.3. Possuir dispositivos redundantes para fornecer energia elétrica e controle de temperatura. Cada um destes dispositivos deve ter capacidade para manter a operação isoladamente em caso de manutenção planejada ou falha.

3.1.1.4.4. Possuir caminhos de distribuição de energia elétrica e conexões de rede local redundantes de modo que um caminho permaneça ativo e o outro possa ser utilizado como alternativa em caso de manutenção planejada ou falha. Os sistemas de distribuição que devem ser considerados nessa especificação são:

3.1.1.4.4.1. Cabine para recebimento de energia externa; 3.1.1.4.4.2. Cabeamento de transmissão de energia; 3.1.1.4.4.3. Quadros de distribuição;

3.1.1.4.4.4. Cabos para conexões de rede;

3.1.1.4.4.5. Possuir múltiplas entradas independentes para fornecimento de energia elétrica. Cada entrada para fornecimento de energia elétrica deve ser capaz de isoladamente suportar a operação do data center;

3.1.1.4.4.6. Possuir múltiplas conexões independentes para acesso à Internet. Cada conexão para acesso à Internet deve ser capaz de isoladamente suportar a operação do data center.

3.1.1.5. A LICITANTE deve possuir ao menos dois SOCs de modo que a indisponibilidade de um deles não afete nenhum aspecto dos serviços prestados. Os SOCs devem estar localizados no Brasil, em cidades diferentes e a no mínimo 50km de distância geodésica um do outro. Cada um deles deve atender aos seguintes requisitos mínimos:

3.1.1.5.1. Estar localizado em prédio comercial que:

3.1.1.5.1.1. Possua gerador de energia para as áreas privativas. O gerador deve ser acionado automaticamente em caso de falta de energia e fornecer energia estabilizada em até 2 minutos após a partida. Os geradores devem suportar a demanda das instalações por até 12 horas sem necessidade de reabastecimento.

3.1.1.5.1.2. Efetue registro dos visitantes com identificação individual e controle digital de entrada e saída.

3.1.1.5.1.3. Possua circuito interno de registro e gravação de imagem em todas as áreas de circulação;

3.1.1.5.1.4. Esteja localizado próximo a vias de grande circulação com acesso imediato a transportes públicos de mais de uma modalidade;

3.1.1.5.2. Funcione em regime 24 x7x365;

3.1.1.5.3. Possua sistema de refrigeração de conforto central.

3.1.1.5.4. Estar conectado aos Data Centers que hospedam os sistemas de suporte técnico, monitoramento, administração e gerenciamento através de múltiplas conexões de rede local ou WAN de forma que a falha de uma conexão isoladamente não afete o acesso aos mesmos;

3.1.1.5.5. Possuir estrutura central para visualização dos painéis dos sistemas de suporte técnico, monitoramento, administração e gerenciamento que permita que todos os profissionais visualizem eventos relevantes simultaneamente.

3.2. EQUIPE

3.2.1. A CONTRATADA deve fornecer pessoal necessário e tecnicamente habilitado à boa e integral execução dos serviços;

3.2.2. A CONTRATADA deve fornecer todos os materiais e serviços próprios e adequados à execução dos trabalhos, competindo-lhe ainda o fornecimento das demais utilidades relacionadas ao cumprimento do objeto deste edital;

3.2.3. A CONTRATADA deve retirar dos serviços qualquer empregado que, a critério do IGEPREV, seja julgado inconveniente ao bom andamento dos trabalhos;

3.2.4. A CONTRATADA deve comunicar, imediatamente, por escrito quaisquer dificuldades encontradas pelos técnicos alocados para execução dos serviços que, eventualmente, possam prejudicar a boa e pontual execução dos trabalhos, sob pena de serem tais dificuldades consideradas inexistentes;

3.2.5. Comprovação, no ato da habilitação, de possuir profissionais com oscertificados abaixo:

Certificação	**Quantidade de Profissionais**
EC-Council/CEH (Certified Ethical Hacker) v6 ou superior	01
PMP – Project Management Professional	01
CISSP (Certified Information System Security Professional) da entidade internacional ISC2	01
Certificação emitida pela fabricante da solução de Firewall Avançado de Próxima Geração	01
Certificação emitida pela fabricante da solução de Gestão de Credenciais Privilegiadas	01
Certificação emitida pela fabricante da solução de Proteção das Estações de Trabalho e Servidores de Rede	01

Tabela 1: Certificações Técnicas

3.2.6. Caso ocorra o desligamento de qualquer um dos profissionais exigidos no item durante a vigência do contrato, a empresa deverá providenciar um substituto, com as mesmas certificações, no prazo máximo de 60 dias.

3.3. EXPERIÊNCIA

3.3.1. A LICITANTE deve possuir atestado(s) de capacidade técnica, focados em prestação de Serviços Gerenciados de Segurança, 24x7x365, onde são ou foram prestados pelo menos os seguintes serviços que compõem o objeto deste Edital: Firewall Próxima Geração e VPN, Proteção das Estações de Trabalho e Servidores de Rede e Gestão de Credenciais Privilegiadas, conferido por empresas públicas ou privadas. O(s) atestado(s) deve(m) comprovar que a(s) rede(s) gerenciada(s) somam, pelo menos, 500 (quinhentos) hosts;

3.3.2. A LICITANTE deve ser parceiro qualificado pela(s) fabricante(s) pelo menos nas seguintes soluções que serão gerenciadas: Firewall Próxima Geração e VPN, Proteção das Estações de Trabalho e Servidores de Rede e Gestão de Credenciais Privilegiadas.

3.4. OUTRAS CARACTERÍSTICAS

3.4.1. Não será permitida a participação de consórcios e sub-locação de serviços em parte ou de modo global.

4. NMS (NÍVEL MÍNIMO DE SERVIÇO)

4.1. Os tempos máximos de resolução especificados devem estar em conformidade com a tabela abaixo e será válida para todos os serviços, sob pena de multa:

4.1.1. Firewall Próxima Geração e VPN, Proteção das Estações de Trabalho e Servidores de Rede e Gestão de Credenciais Privilegiadas

Atividade	Tempo de Resolução Máximo
Alteração e inclusão de regras	60 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Alteração de configurações	60 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção
Atualização (implementação de patches e fixes)	24 horas após liberação do pacote pelo fabricante, condicionado à homologação pela CONTRATADA e liberação de janela de mudança pelo IGEPREV
Início de atuação remota para resolução de problemas	60 minutos após abertura de chamado ou detecção pelo SOC
Início da atuação local para resolução de problemas e troca de equipamentos	6 horas após abertura de chamado ou detecção pelo SOC

Atividade	Tempo de Resolução Máximo
Implementação de novos serviços ou dispositivos	24 horas após abertura de chamado no Response Team
Relatório Periódico Técnico	Mensal
Relatório emergencial	24 horas após o evento, desde que solicitado pelo IGEPREV

Tabela 2: NMS para os serviços

4.2. Os NMSs, especificados na tabela acima, podem ser revisados 1 (um) ano após a assinatura do contrato, caso o IGEPREV entenda que os tempos aqui especificados não estão atendendo as suas necessidades, sujeito à aceitação da CONTRATADA.

5. DESCRIÇÃO DOS NÍVEIS DE SERVIÇOS REQUERIDOS

5.1. Para todos os serviços que fazem parte deste Termo de Referência deverão ter:

5.1.1. Disponibilidade de serviço mensal de no mínimo 99% (noventa e nove por cento). Este percentual será calculado da seguinte forma:

5.1.1.1. Apura-se a quantidade de horas de indisponibilidade no mês;

5.1.1.2. Apura-se a quantidade de horas de disponibilidade do mês;

5.1.1.3. Subtrai-se o número de horas de disponibilidade no mês pelo número de horas de indisponibilidade no mês;

5.1.1.4. Divide-se o valor obtido no item anterior pelo número de horas de disponibilidade no mês;

5.1.1.5. Multiplica-se o valor obtido no item anterior por 100 (cem).

5.2. Não serão consideradas indisponibilidade as seguintes situações:

5.2.1. Falta de energia no local de instalação da solução;

5.2.2. Indisponibilidade da rede lógica à qual esteja instalado equipamento da solução;

5.2.3. Manutenções programadas pela CONTRATADA ou pelo IGEPREV com aceite dado em documento pela parte requerida.

5.3. O tempo máximo de manutenções, por serviço gerenciado implantado, programadas pela CONTRATADA, não deverá ultrapassar 4 (quatro) horas mês e 24 (vinte e quatro) horas ano. Estes tempos referem-se a um equipamento ou conjunto de equipamentos de uma solução (Exemplo: cluster – dois ou mais equipamentos ou fail-over).

5.4. Todos os serviços cujo NMS (Nível Mínimo de Serviço) fazem parte do objeto deste Termo de Referência deverão ter meta de atendimento de, no mínimo, 95% (noventa e cinco por cento).

Este percentual será calculado, por serviço, da seguinte forma:

5.4.1. Apura-se o número de chamados de serviço atendidos dentro do NMS no mês;

5.4.2. Apura-se o número de chamados de serviço atendidos fora do NMS no mês;

5.4.3. Subtrai-se o número de chamados do serviço atendidos dentro do NMS no mês pelo número de chamados do serviço atendidos fora do NMS no mês;

5.4.4. Divide-se o valor obtido no item anterior pelo número de chamados de serviço no mês;

5.4.5. Multiplica-se o valor obtido no item anterior por 100 (cem).

5.5. DESCONTOS PELO NÃO CUMPRIMENTO DOS SLAS ESPECIFICADOS E ATRASOS NA FASE DE IMPLANTAÇÃO:

5.5.1. Ao final do mês, será computado o percentual de atendimento ao NMS conforme definido no item 4 – Descrição dos Níveis de Serviço Requeridos.

5.5.2. Caso o nível de atendimento do SLA seja inferior a 95% (noventa e cinco por cento), será aplicado desconto de 15% (quinze por cento) na nota fiscal/fatura dos serviços;

5.5.3. Caso o percentual de atendimento esteja compreendido entre 95% e 96.99%, será aplicado desconto de 5% (cinco por cento) na nota fiscal/fatura dos serviços;

5.5.4. Caso o percentual de atendimento esteja compreendido entre 97% e 97.99%, será aplicado desconto de 3% (três por cento) na nota fiscal/fatura dos serviços;

5.5.5. Pelo fechamento não autorizado de chamados técnicos:

5.5.5.1. Os chamados abertos somente poderão ser fechados após autorização de funcionário designado pelo IGEPREV. Caso haja fechamento de chamados, por parte da contratada, que não tenha sido previamente autorizado pelo IGEPREV, será cobrada uma multa de 0,5% (zero vírgula cinco por cento) no valor mensal do serviço, por chamado fechado sem autorização, cumulativamente.

5.5.6. Pelo não cumprimento do índice de disponibilidade do serviço:

5.5.6.1. Será computado como indisponibilidade todo o tempo decorrido entre o início da interrupção do serviço e sua total recuperação;

5.5.6.2. Ao final do mês, será computado o tempo total de indisponibilidade do serviço, conforme definido no item 5 - DESCRIÇÃO DOS NÍVEIS DE SERVIÇOS REQUERIDOS, sendo cobrada uma multa de 0,5% (zero vírgula cinco por cento) no valor mensal do serviço por hora ou fração que exceder ao limite estabelecido para o serviço. Caso haja mais de um serviço em que o tempo total de disponibilidade ficou fora do limite estabelecido de tolerância, será aplicada, adicionalmente, multa de 1% (um por cento) no valor mensal do serviço, cumulativamente;

6. ESPECIFICAÇÕES TÉCNICAS

6.1. A Solução Integrada de Serviços Gerenciados de Segurança deverá englobar alocação de equipamentos, produtos, peças e softwares necessários à perfeita execução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos produtos e softwares utilizados e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

6.2. A prestação dos serviços será baseada no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas e qualitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) definido em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços. Os níveis mínimos de serviços contratados, presentes no Nível Mínimo de Serviço destas especificações técnicas, serão registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar os pagamentos previstos.

6.3. O modelo de prestação de serviço conterá, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo IGEPREV, tais como abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas periodicamente pela CONTRATADA *in-loco*, tais como análise de vulnerabilidades de segurança e monitoração das ferramentas utilizadas nos serviços.

6.4. Os serviços constantes no objeto deste Termo de Referência estão subdivididos conforme a Tabela 12 que segue:

Item	Descrição	Quantidade	Meses
1	Serviço de Proteção de Perímetro com Firewall Avançado de Próxima Geração	1	36
2	Serviços de Proteção das Estações de Trabalho e Servidores de Rede	1	36
3	Serviço de Gestão de Credenciais Privilegiadas	1	36
4	Serviços Técnicos Especializados	4.000 horas	

Tabela 3: Escopo de Serviços – Detalhamento

6.4.1. O Item 1 refere-se ao Serviço de "**Firewall de Proteção de Perímetro com Firewall Avançado de Próxima Geração**", provido por um Cluster de, pelo menos, dois equipamentos, capazes de regular o tráfego de dados entre as distintas redes do IGEPREV e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra. Os equipamentos deverão implementar tecnologias de filtro de pacotes *Stateful Inspection*, utilizando mecanismos de verificação de tráfego segundo tabela de estado de conexões. Além disso, os equipamentos do cluster deverão ser capazes de implementar recursos de criptografia para tunelamento em redes inseguras de comunicação, tal como a Internet, por meio de redes privadas

virtuais (VPN), garantindo confidencialidade, autenticação e integridade necessárias para a segurança do tráfego de dados do IGEPREV.

6.4.2. O Item 2 trata dos "***Serviços de Proteção das Estações de Trabalho e Servidores de Rede***", responsáveis por proteger o ambiente computacional do IGEPREV contra *malwares* (Trojans, Virus, Worms, Spywares e demais ameaças), ataques, pacotes indesejados e controle dos dispositivos inseridos nas estações de Trabalho e Servidores de Rede, este com versões específicas para ambiente virtualizado, compatível com *VMWARE*. A Solução deverá possuir capacidade de informar sites maliciosos e até autorizar e/ou bloquear o acesso e possuir centro de inteligência capaz de informar reputação de arquivos.

6.4.3. O Item 3 trata do "***Serviço de Gestão de Credenciais Privilegiadas***" responsável por proteger contas privilegiadas que quando mal utilizadas expõe a vulnerabilidades graves e diversas para uma organização. Elas são utilizadas para manter ambientes, armazenar dados sensíveis e sobretudo garantir a continuidade de qualquer negócio. Quando exploradas por um atacante, pode ocorrer de sistemas serem desabilitados, a tomada do controle por parte do atacante de toda infraestrutura de tecnologia e o acesso a dados mais sensíveis existentes na organização. A solução deverá gerir, portanto, as credenciais mais importantes do ambiente, através de um cofre digital (com rotação de senhas automáticas e outros benefícios), auditoria, gravação de sessões e políticas de acesso e comandos dos usuários que possuem acessos a elementos e serviços chaves da organização.

6.4.4. O item 4 trata de ***Serviços Técnicos Especializados*** em segurança da informação e infraestrutura que por algum motivo estejam inerentes para a sustentação da segurança lógica, com métrica baseada em horas de serviço, compreendendo a execução de atividades de elaboração de pareceres e planos, análise de ambiente e de ativos, auditoria forense, mudança de endereço de unidades do IGEPREV (aspectos de segurança) e alteração de arquitetura do ambiente computacional e da infraestrutura de segurança do IGEPREV. Consiste em atividades a serem demandadas por meio da celebração prévia de ordens de serviço, com total de horas definido previamente, de comum acordo entre o IGEPREV e a contratada, cujo pagamento será efetivado somente após entrega de relatório de prestação de serviços e recebimento por parte do IGEPREV.

7. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados referentes aos itens 1 a 3 do objeto. Os termos "possui", "permite", "suporta" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

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. Já os softwares comerciais deverão, ainda, ser instalados em sua versão mais atualizada e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou softwares utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança e mantenham-se todos os módulos propostos integrados entre si, ou seja, trocando informações entre os módulos deste termo de Referência, simplificando a gestão e minimizando os riscos a segurança do IGEPREV.

Ademais, todos os componentes necessários à prestação dos serviços deverão ser integráveis entre si, mantendo-se como uma única solução sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do IGEPREV.

7.1. SERVIÇO DE FIREWALL PRÓXIMA GERAÇÃO E VPN

7.1.1. Características gerais da Solução:

7.1.1.1. Toda Solução de segurança proposta deverá ser fornecida por um único fabricante de modo que tanto o suporte da solução quanto as funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console de gerenciamento.

7.1.2. Características mínimas de hardware por equipamento (*Appliance*)

7.1.2.1. Throughput de, no mínimo, 15 Gbps com a funcionalidade de firewall habilitada para tráfego IPv4 e IPv6, independente do tamanho do pacote;
7.1.2.2. Throughput de, no mínimo, 2 Gbps com a funcionalidade de IPShabilitada;
7.1.2.3. Throughput de, no mínimo, 1 Gbps com a funcionalidade de NGFWhabilitada;
7.1.2.4. Suporte a, no mínimo, 1M conexões simultâneas;
7.1.2.5. Suporte a, no mínimo, 50K novas conexões por segundo;
7.1.2.6. Throughput de, no mínimo, 10 Gbps de VPN IPSec;
7.1.2.7. Estar licenciado para, ou suportar sem o uso de licença, 2K túneis de VPN IPSEC Site-to-Site simultâneos;
7.1.2.8. Estar licenciado para, ou suportar sem o uso de licença, 10K túneis de clientes VPN IPSEC simultâneos;
7.1.2.9. Throughput de, no mínimo, 750 Mbps de VPN SSL;
7.1.2.10. Suporte a, no mínimo, 400 clientes de VPN SSL simultâneos;
7.1.2.11. Suportar no mínimo 2 Gbps de throughput de IPS;
7.1.2.12. Suportar no mínimo 750 Mbps de throughput de Inspeção SSL;
7.1.2.13. Throughput de, no mínimo, 900 Mbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, Antivírus e

Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;
7.1.2.14. Permitir gerenciar ao menos 64 Access Points;
7.1.2.15. Possuir ao menos 12 interfaces 1Gbps RJ-45;
7.1.2.16. Possuir ao menos 2 interfaces 1Gbps SFP;
7.1.2.17. Possuir ao menos 2 interfaces 10Gbps SFP+;
7.1.2.18. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance;
7.1.2.19. Suporte a, no mínimo, 10 sistemas virtuais lógicos (Contextos) por appliance.

7.1.3. Requisitos Mínimos de Funcionalidade - Características Gerais

7.1.3.1. A solução deve consistir em plataforma de proteção de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;
7.1.3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
7.1.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
7.1.3.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
7.1.3.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;
7.1.3.6. A gestão do equipamento deve ser compatível através da interface de gestão Web no mesmo dispositivo de protecção da rede;
7.1.3.7. Os dispositivos de proteção de rede devem possuir suporte a 4094 VLAN Tags 802.1q;
7.1.3.8. Os dispositivos de proteção de rede devem possuir suporte a agregação de links 802.3ad e LACP;
7.1.3.9. Os dispositivos de proteção de rede devem possuir suporte a Policy based routing ou policy based forwarding;
7.1.3.10. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
7.1.3.11. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
7.1.3.12. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
7.1.3.13. Os dispositivos de proteção de rede devem suportar sFlow;
7.1.3.14. Os dispositivos de proteção de rede devem possuir suporte a Jumbo Frames;
7.1.3.15. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
7.1.3.16. Deve suportar NAT dinâmico (Many-to-1);
7.1.3.17. Deve suportar NAT dinâmico (Many-to-Many);
7.1.3.18. Deve suportar NAT estático (1-to-1);
7.1.3.19. Deve suportar NAT estático (Many-to-Many);
7.1.3.20. Deve suportar NAT estático bidirecional 1-to-1;
7.1.3.21. Deve suportar Tradução de porta (PAT);
7.1.3.22. Deve suportar NAT de Origem;
7.1.3.23. Deve suportar NAT de Destino;

7.1.3.24. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
7.1.3.25. Deve poder combinar NAT de origem e NAT de destino na mesma politica;
7.1.3.26. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
7.1.3.27. Deve suportar NAT64 e NAT46;
7.1.3.28. Deve implementar o protocolo ECMP;
7.1.3.29. Deve suportar SD-WAN de forma nativa;
7.1.3.30. Deve implementar balanceamento de link por hash do IP de origem;
7.1.3.31. Deve implementar balanceamento de link por hash do IP de origem e destino;
7.1.3.32. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links;
7.1.3.33. Deve suportar o balanceamento de, no mínimo, três links;
7.1.3.34. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
7.1.3.35. Deve permitir monitorar via SNMP falhas de hardware, uso de recursos por número elevado de sessões, conexões por segundo, número de túneis estabelecidos na VPN, CPU, memória, status do cluster, ataques e estatísticas de uso das interfaces de rede;
7.1.3.36. Enviar log para sistemas de monitoração externos, simultaneamente;
7.1.3.37. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
7.1.3.38. Proteção anti-spoofing;
7.1.3.39. Implementar otimização do tráfego entre dois equipamentos;
7.1.3.40. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
7.1.3.41. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
7.1.3.42. Suportar OSPF graceful restart;
7.1.3.43. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
7.1.3.44. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
7.1.3.45. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
7.1.3.46. Deve suportar Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
7.1.3.47. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em modo transparente;
7.1.3.48. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em layer 3;
7.1.3.49. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo em layer 3 e com no mínimo 3 equipamentos no cluster;
7.1.3.50. A configuração em alta disponibilidade deve sincronizar sessões;
7.1.3.51. A configuração em alta disponibilidade deve sincronizar configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;

7.1.3.52. A configuração em alta disponibilidade deve sincronizar associações de Segurança das VPNs;
7.1.3.53. A configuração em alta disponibilidade deve sincronizar tabelas FIB;
7.1.3.54. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
7.1.3.55. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance;

7.1.3.56. Em alta disponibilidade, deve ser possível o uso de clusters virtuais, seja ativo- ativo ou ativo-passivo, permitindo a distribuição de carga entre diferentes contextos;
7.1.3.57. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
7.1.3.58. O gerenciamento da solução deve suportar acesso via SSH e interface WEB (HTTPS), incluindo, mas não limitado à, exportar configuração dos sistemas virtuais (contextos) por ambas interfaces;
7.1.3.59. Controle, inspeção e descriptografia de SSL para tráfego de entrada (Inbound) e Saída (Outbound), sendo que deve suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
7.1.3.60. Deve suportar uma abordagem de segurança integrada para fornecer uma solução de segurança holística abrangendo toda a rede;
7.1.3.61. Essa abordagem de segurança integrada deve identificar potenciais vulnerabilidades e destacar as melhores práticas que poderiam ser usadas para melhorar a segurança e o desempenho geral de uma rede;
7.1.3.62. Deve existir um Serviço de Suporte que oferece aos clientes uma verificação de saúde recorrente com um relatório de auditoria mensal personalizado de seus appliances NGFW;
7.1.3.63. A console de administração deve suportar no mínimo, inglês, Espanhol e Português;
7.1.3.64. A console deve suportar a administração de switches e rádios sem-fio para melhorar o nível de segurança;
7.1.3.65. A solução deve suportar integração nativa de equipamentos de proteção de correio eletrônico, firewall de aplicação, proxy, cache e ameaças avançadas.

7.1.3.66. Controle por Politica de Firewall

7.1.3.67. Deverá suportar controles por zona de segurança;
7.1.3.68. Controles de políticas por porta e protocolo;
7.1.3.69. Controle de políticas por aplicações, grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações;
7.1.3.70. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
7.1.3.71. Firewall deve ser capaz de aplicar a inspeção UTM (Application Control e Webfiltering no mínimo) diretamente às políticas de segurança versus viaperfis;
7.1.3.72. Além dos endereços e serviços de destino, objetos de serviços de Internet devem poder ser adicionados diretamente às políticas de firewall;
7.1.3.73. Deve suportar automatização de situações como detecção de equipamentos comprometidos, estado do sistema, mudança de configuração, eventos específicos e aplicar uma ação que pode ser notificação, bloqueio de um equipamento, execução de scripts ou funcionamento em nuvem pública;
7.1.3.74. Deve suportar o padrão de indústria 'syslog' protocol para armanazemento usando o formato Common Event Format (CEF);
7.1.3.75. Deve haver uma maneira de assegurar que o almazenamento dos logs em tempo real não superam a velocidade de upload;

7.1.3.76. Deve suportar o protocolo padrão da indústria VXLAN;
7.1.3.77. A solução deve permitir a implementação sem assistência de SD-WAN;
7.1.3.78. No SD-WAN deve suportar QoS, modelagem de tráfico, rota por políticas, IPSEC VPN;
7.1.3.79. A solução deve suportar a integração nativa com solução de sandboxing, proteção de correio electrônico, cache e Web application firewall;

7.1.3.80. Controle de Aplicações

7.1.3.81. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
7.1.3.82. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado a: tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
7.1.3.83. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
7.1.3.84. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
7.1.3.85. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
7.1.3.86. Identificar o uso de táticas evasivas via comunicações criptografadas;
7.1.3.87. Atualizar a base de assinaturas de aplicações automaticamente;
7.1.3.88. Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos;
7.1.3.89. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;
7.1.3.90. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;
7.1.3.91. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
7.1.3.92. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
7.1.3.93. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
7.1.3.94. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo;
7.1.3.95. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
7.1.3.96. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Tecnologia utilizada nas aplicações (Client- Server, Browse Based, Network Protocol, etc);

7.1.3.97. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação;
7.1.3.98. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
7.1.3.99. Deve ser possível configurar Application Override permitindo selecionar aplicações individualmente;

7.1.3.100. Prevenção de Ameaças

7.1.3.101. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
7.1.3.102. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
7.1.3.103. As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
7.1.3.104. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
7.1.3.105. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
7.1.3.106. Deve permitir o bloqueio de vulnerabilidades;
7.1.3.107. Deve incluir proteção contra ataques de negação de serviços;
7.1.3.108. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise de decodificação de protocolo;
7.1.3.109. Deverá possuir o seguinte mecanismos de inspeção de IPS: Análise para detecção de anomalias de protocolo;
7.1.3.110. Deverá possuir o seguinte mecanismos de inspeção de IPS: IP Defragmentation;
7.1.3.111. Deverá possuir o seguinte mecanismos de inspeção de IPS: Remontagem de pacotes de TCP;
7.1.3.112. Deverá possuir o seguinte mecanismos de inspeção de IPS: Bloqueio de pacotes malformados;
7.1.3.113. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
7.1.3.114. Detectar e bloquear a origem de portscans;
7.1.3.115. Bloquear ataques efetuados por worms conhecidos;
7.1.3.116. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
7.1.3.117. Possuir assinaturas para bloqueio de ataques de buffer overflow;
7.1.3.118. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
7.1.3.119. Identificar e bloquear comunicação com botnets;
7.1.3.120. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
7.1.3.121. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

7.1.3.122. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
7.1.3.123. Os eventos devem identificar o país de onde partiu a ameaça;
7.1.3.124. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
7.1.3.125. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
7.1.3.126. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por usuários, Grupos de usuário, origem, destino, zonas de segurança;
7.1.3.127. Caso o firewall possa ser coordenado por software de segurança do computador do usuário final (laptop, desktop, etc.) deve ter um perfil onde se possa executar a análise de vulnerabilidade nestes equipamentos de usuário e assegurar que estes execute versões compatíveis;
7.1.3.128. Fornecem proteção contra ataques de dia zero por meio de estreita integração com os componentes Security Fabric, incluindo NGFW, Sandbox (on-premise e nuvem);

7.1.3.129. Filtro de URL

7.1.3.130. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
7.1.3.131. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local, em modo de proxy transparente e explícito;
7.1.3.132. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
7.1.3.133. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
7.1.3.134. Possuir pelo menos 60 categorias de URLs;
7.1.3.135. Deve possuir a função de exclusão de URLs do bloqueio, por categoria;
7.1.3.136. Permitir a customização de página de bloqueio;
7.1.3.137. Permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site);
7.1.3.138. Além do Explicit Web Proxy, suportar proxy Web transparente;

7.1.3.139. Identificação de Usuários

7.1.3.140. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

7.1.3.141. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
7.1.3.142. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários ou qualquer tipo de restrição de uso como, mas não limitado à, utilização de sistemas virtuais, segmentos de rede, etc;
7.1.3.143. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
7.1.3.144. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;
7.1.3.145. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall(Captive Portal);
7.1.3.146. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
7.1.3.147. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
7.1.3.148. Permitir integração com tokens para autenticação dos usuários, incluindo, mas não limitado a acesso a internet e gerenciamento da solução;
7.1.3.149. Prover no mínimo um token nativamente, possibilitando autenticação de duplo fator;

7.1.3.150. QoS e Traffic Shaping

7.1.3.151. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube, Ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máxima largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
7.1.3.152. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
7.1.3.153. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
7.1.3.154. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
7.1.3.155. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
7.1.3.156. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
7.1.3.157. O QoS deve possibilitar a definição de tráfego com banda garantida;
7.1.3.158. O QoS deve possibilitar a definição de tráfego com banda máxima;
7.1.3.159. O QoS deve possibilitar a definição de fila de prioridade;
7.1.3.160. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
7.1.3.161. Suportar modificação de valores DSCP para o Diffserv;

7.1.3.162. Suportar priorização de tráfego usando informação de Type of Service;
7.1.3.163. Deve suportar QOS (traffic-shapping), em interface agregadas ou redundantes;

7.1.3.164. Filtro de Dados

7.1.3.165. Permitir a criação de filtros para arquivos e dados pré-definidos;
7.1.3.166. Os arquivos devem ser identificados por extensão e tipo;
7.1.3.167. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
7.1.3.168. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
7.1.3.169. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
7.1.3.170. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

7.1.3.171. Geo Localização

7.1.3.172. Suportar a criação de políticas por geo-localização, permitindo o trafego de determinado Pais/Países sejam bloqueados;
7.1.3.173. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
7.1.3.174. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas;
7.1.3.175. VPN
7.1.3.176. Suportar VPN Site-to-Site e Cliente-To-Site;
7.1.3.177. Suportar IPSec VPN;
7.1.3.178. Suportar SSL VPN;
7.1.3.179. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
7.1.3.180. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
7.1.3.181. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
7.1.3.182. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
7.1.3.183. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
7.1.3.184. Suportar VPN em em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
7.1.3.185. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
7.1.3.186. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
7.1.3.187. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
7.1.3.188. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

7.1.3.189. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
7.1.3.190. Deverá manter uma conexão segura com o portal durante a sessão;
7.1.3.191. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

7.1.3.192. Wireless Controller

7.1.3.193. Deverá administrar e controlar de maneira centralizada os pontos de acesso wireless do mesmo fabricante da solução ofertada;
7.1.3.194. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
7.1.3.195. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac e que transmitam tráfego IPv4 e IPv6 através do controlador;
7.1.3.196. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor;
7.1.3.197. O controlador wireless deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
7.1.3.198. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
7.1.3.199. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
7.1.3.200. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes devem ser tunelados até o controlador wireless;
7.1.3.201. Quando tunelado, o tráfego deve ser criptografado através de DTLS ou IPSEC;
7.1.3.202. Deve permitir o gerenciamento de pontos de acesso conectados remotamente através de links WAN. Neste cenário o encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma distribuída (local switching), ou seja, o tráfego deve ser comutado localmente na interface LAN do ponto de acesso e não necessitará de tunelamento até o controlador wireless;
7.1.3.203. Quando o encaminhamento do tráfego for distribuído (local switching) e a autenticação via PSK, caso haja falha na comunicação entre os pontos de acesso e o controlador wireless, os usuários associados devem permanecer associados aos pontos de acesso e ao mesmo SSID. Deve ser possível ainda permitir a conexão de novos usuários à rede wireless;
7.1.3.204. A solução deve permitir definir quais redes serão tuneladas até a controladora e quais redes serão comutadas diretamente pela interface do ponto de acesso;
7.1.3.205. A solução deve suportar recurso de Split-Tunneling de forma que seja possível definir, através das subredes de destino, quais pacotes serão tunelados até a controladora e quais serão comutados locamente na interface do ponto de acesso;
7.1.3.206. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

7.1.3.207. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado dBm;
7.1.3.208. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
7.1.3.209. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
7.1.3.210. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interfaceWLAN;
7.1.3.211. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off- channel/Background scanning. Quando realizada através de Off- channel/Background scanning, a solução deve ser capaz de identificar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
7.1.3.212. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexbilidade no design da rede wireless;
7.1.3.213. A solução deve permitir a adição de controlador redundante operando em N+1. Neste modo, o controlador redundante deve monitorar a disponibilidade e sincronizar as configurações do principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
7.1.3.214. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
7.1.3.215. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
7.1.3.216. A solução deve garantir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
7.1.3.217. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
7.1.3.218. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
7.1.3.219. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
7.1.3.220. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento

de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

7.1.3.221. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

7.1.3.222. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

7.1.3.223. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

7.1.3.224. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

7.1.3.225. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

7.1.3.226. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados para as frequências de 2.4 e 5GHz e padrões 802.11a/b/g/n/ac;

7.1.3.227. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

7.1.3.228. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

7.1.3.229. A solução deve permitir a configuração do valor de Short Guard Interval para 802.11n e 802.11ac em 5GHz;

7.1.3.230. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime alocando porcentagens a serem utilizadas nos SSIDs;

7.1.3.231. A solução deve implementar regras de firewall (stateful) para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que deve usar como critério endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

7.1.3.232. solução deve implementar recurso de web filtering para controle de websites acessados na rede wireless. Deve possuir uma base de conhecimento para categorização dos sites e permitir configurar quais categorias de sites serão permitido e bloqueados para cada perfil de usuário e SSID;

7.1.3.233. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle. Deve permitir o funcionamento deste recurso e a atualização periódica da base de aplicações durante todo o período de garantia da solução;

7.1.3.234. A base de reconhecimento de aplicações através de DPI deve identificar com, no mínimo, 1500 (mil e quinhentas) aplicações;

7.1.3.235. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI;
7.1.3.236. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS;
7.1.3.237. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados:

7.1.3.237.1. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding) 7.1.3.237.2. Association Flood
7.1.3.237.3. Authentication Flood
7.1.3.237.4. Broadcast Deauthentication
7.1.3.237.5. Spoofed Deauthentication;
7.1.3.237.6. ASLEAP;
7.1.3.237.7. Null Probe Response / Null SSID Probe Response; 7.1.3.237.8. Long Duration;
7.1.3.237.9. Ataques contra Wireless Bridges; 7.1.3.237.10.Weak WEP;
7.1.3.237.11.Invalid MAC OUI.

7.1.3.238. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication;
7.1.3.239. A solução deve implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede wireless;
7.1.3.240. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes wireless;
7.1.3.241. Permitir configurar o bloqueio na comunicação entre os clientes wireless conectados a um determinado SSID;
7.1.3.242. Deve implementar autenticação administrativa através do protocolo RADIUS;
7.1.3.243. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
7.1.3.244. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
7.1.3.245. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;
7.1.3.246. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;
7.1.3.247. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
7.1.3.248. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
7.1.3.249. A solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
7.1.3.250. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede;

7.1.3.251. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
7.1.3.252. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
7.1.3.253. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
7.1.3.254. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
7.1.3.255. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
7.1.3.256. A solução deve garantir que usuários se autentiquem em captive portal que faça uso de endereço IPv6;
7.1.3.257. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
7.1.3.258. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
7.1.3.259. A solução deve implementar recurso de DHCP Server (IPv4 e IPv6) para facilitar a configuração de redes visitantes;
7.1.3.260. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispostivo conectado à rede wireless;
7.1.3.261. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
7.1.3.262. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
7.1.3.263. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
7.1.3.264. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
7.1.3.265. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
7.1.3.266. A solução deve permitir ser gerenciada através do protocolo SNMP (v1, v2c e v3), além de emitir notificações através da geração de traps;
7.1.3.267. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
7.1.3.268. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
7.1.3.269. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
7.1.3.270. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
7.1.3.271. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

7.1.3.272. A solução deve implementar o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
7.1.3.273. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
7.1.3.274. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização individualizada através da interface gráfica;
7.1.3.275. A solução deve possuir ferramentas de diagnósticos e debug;
7.1.3.276. A solução deve suportar comunicação com elementos externos através de APIs;
7.1.3.277. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

7.2. SOLUÇÃO DE PROTEÇÃO DAS ESTAÇÕES DE TRABALHO E SERVIDORES DE REDE

7.2.1. Características Gerais da Solução

7.2.1.1. Toda a Solução de segurança proposta deverá ser fornecida por um único fabricante de modo que tanto o suporte da solução quanto as funcionalidades sejam inteiramente integradas e gerenciadas através de uma única console degerenciamento.

7.2.1.2. Solução de Segurança para Servidores de Rede (físicos e virtuais)

7.2.1.2.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:

- Windows Server 2003 (32-bit/64-bit)
- Windows Server 2008 (32-bit/64-bit), 2008 R2, 2012, 2012 R2, 2012 Server Core (64-bit)
- Windows Server 2016 (64-bit)
- Red Hat Enterprise 5, 6, 7 (32-bit/64-bit)
- SUSE Enterprise 10, 11, 12 (32-bit/64-bit)
- CentOS 5, 6,7 (32-bit/64-bit)
- Ubuntu 10, 12, 14 (64-bit)
- Debian 6, 7, 8 (64-bit)
- Oracle Solaris 9, 10, 11 (64-bit SPARC), 10, 11 (64-bit x86)
- AIX 5.3, 6.1, 7.1 e
- HP-UX 11i v3 (11.31)

7.2.1.2.2. A solução deverá ser totalmente compatível e homologada com o ambiente Vmware: VMware® vSphere: 5.5/6.0, View 4.5/5.0/5.1, ESX 5.5, 6.2.X, 6.5, NSX 6.2.X, 6.3
7.2.1.2.3. A solução deverá permitir a integração com VMware vSphere 6 e com NSX estendendo os benefícios da micro-segmentação em um datacenter definido por software e fazendo com que as políticas de segurança estejam atreladas às Vms onde quer que elas estejam;
7.2.1.2.4. A solução deverá permitir a integração com Vmware Vrealize para o monitoramento do ambiente;

7.2.1.2.5. A solução deverá permitir a integração com pelo menos as seguintes plataforma de nuvem: Vmware Vcloud, Ms Azzure e AWS;
7.2.1.2.6. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
7.2.1.2.7. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;
7.2.1.2.8. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer e Firefox. Deve ainda suportar certificado digital para gerenciamento;
7.2.1.2.9. A console de administração deverá permitir o envio de notificações via SMTP;
7.2.1.2.10. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
7.2.1.2.11. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas.
7.2.1.2.12. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos.
7.2.1.2.13. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
7.2.1.2.14. A solução deverá permitir a criação de múltiplos perfis de segurança, que serão vinculados aos diferentes tipos de servidores do ambiente;
7.2.1.2.15. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;
7.2.1.2.16. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF e RTF.
7.2.1.2.17. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
7.2.1.2.18. A solução deverá prover relatórios contendo no mínimo as sequintes informações; malware, regras de IPS e Firewall.
7.2.1.2.19. A console de gerenciamento deve armazenar políticas e logs em base de dados. A escolha da base de dados pode ser facultativa entre Oracle e SQL.
7.2.1.2.20. A console de gerenciamento deve apresentar alta disponibilidade de modo que na ausência da principal os clientes automaticamente se comuniquem com a secundária e todas as configurações devem permanecer;
7.2.1.2.21. Quando operando em modo alta disponibilidade, ambos os consoles devem compartilhar a mesma database;
7.2.1.2.22. A console deve se integrar com o Active Directory para que os usuários do Active Directory possam administrar a solução de acordo com as permissões;
7.2.1.2.23. A console deve se integrar com o Active Directory para que possa ser efetuado o controle das máquinas no Active Directory;
7.2.1.2.24. Para efeito de administração, deve ser possível de se replicar a estrutura do Active Directory na console de administração;
7.2.1.2.25. A solução de segurança para data center deverá suportar Docker para proteger os containers;

7.2.1.2.26. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
7.2.1.2.27. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;
7.2.1.2.28. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
7.2.1.2.29. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
7.2.1.2.30. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
7.2.1.2.31. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL com o servidor de onde ela buscará as informações;
7.2.1.2.32. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;
7.2.1.2.33. Os agentes para plataforma Linux deverão ser instalador por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente;
7.2.1.2.34. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;
7.2.1.2.35. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
7.2.1.2.36. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts; 7.2.1.2.37. A solução deverá vir com perfis default pré-definidos e aptos a funcionarem de
acordo com sua denominação;
7.2.1.2.38. Deverá possuir uma hierarquia de prevalecimento de configurações, seguindo no mínimo a ordem: Global -> Perfis -> hosts;
7.2.1.2.39. A solução deverá mostrar quais máquinas estão usando determinada política. 7.2.1.2.40. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde
estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
7.2.1.2.41. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
7.2.1.2.42. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
7.2.1.2.43. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
7.2.1.2.44. Também deverá ser possível realizar o rastreamento por portas abertas, identificando possíveis serviços ativos e escutando;

7.2.1.2.45. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
7.2.1.2.46. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
7.2.1.2.47. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
7.2.1.2.48. A solução deverá ter a capacidade de se integrar com os principais softwares de SIEMs, no mínimo com: IBMQradar, HPArcSight, RSA Envision e NetIQ de modo a permitir enviar os seus logs para essas soluções;
7.2.1.2.49. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers; 7.2.1.2.50. A solução deverá ter a possibilidade de enviar eventos da console via SNMP; 7.2.1.2.51. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
7.2.1.2.52. A solução deverá permitir exportar relatórios para no mínimo os formatos PDF e RTF;
7.2.1.2.53. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
7.2.1.2.54. A lista de contatos de recebimento de relatório poderá ser obtida através do Active Directory;
7.2.1.2.55. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
7.2.1.2.56. Após a atualização deve ser informado o que foi modificado ou adicionado; 7.2.1.2.57. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não distribuí-las aos clientes;
7.2.1.2.58. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;
7.2.1.2.59. A solução deverá ter capacidade de gerar pacote de auto diagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
7.2.1.2.60. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
7.2.1.2.61. No gerenciamento de licenças, deve ser informada quantidade LICITANTE e quantidade em utilização de clientes;
7.2.1.2.62. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
7.2.1.2.63. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;
7.2.1.2.64. Possibilidade de customizar a escolha do serviço de Whois para a identificação dos IPs que estejam realizando ataques;
7.2.1.2.65. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
7.2.1.2.66. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

7.2.1.2.67. A console de gerenciamento deve se integrar com o Vmware vCenter 4.0 ou Superior, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
7.2.1.2.68. A partir desta integração, deverá ser possível gerir a segurança dos guests vm, podendo ser atribuídos perfis de segurança, regras únicas para cada host, além de possibilitar a coleta dos logs gerados para cada módulo habilitado.
7.2.1.2.69. Esta integração deve possibilitar que, a partir da instalação e integração de um virtual appliance do fabricante da solução de segurança com o ambiente Vmware e suas APIs, seja possível proteger as guests VMs sem a necessidade de instalação de agentes de segurança do fabricante da solução nas guests VMs.
7.2.1.2.70. Este virtual appliance deverá permitir integração com as seguintes APIs VMware: Vmsafe API e vShield Endpoint API, possibilitando que funcionalidades de Firewall, Proteção de Aplicações Web, Antimalware, Controle de Acesso a Sites Maliciosos, Monitoramento de Integridade de Arquivos, Controle de Aplicações e IDS/IPS, possam ser efetuados diretamente via hypervisor e virtual appliance em conjunto, não necessitando a instalação de agentes adicionais de segurança do fabricante nos guests VMsprotegidos;
7.2.1.2.71. A solução deverá ser capaz de implementar as funcionalidades de Antimalware, Controle de Acesso a Sites Maliciosos, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Windows através de um único agente;
7.2.1.2.72. A solução deverá ser capaz de implementar as funcionalidades de Antimalware, Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Linux através de um único agente;
7.2.1.2.73. A solução deverá ser capaz de implementar as funcionalidades de Firewall, IDS/IPS, Controle de Aplicações, Proteção de aplicações Web, Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais Solaris através de um único agente;
7.2.1.2.74. A solução deverá ser capaz de implementar as funcionalidades de Inspeção de Logs e Monitoramento de Integridade nos sistemas operacionais HP-UX e AIX através de um único agente;
7.2.1.2.75. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
7.2.1.2.76. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
7.2.1.2.77. A solução deverá ser possuir no mínimo as seguintes certificações de validação e/ou compatibilidade com padrões de mercado:
7.2.1.2.78. Certified Red Hat Ready 7.2.1.2.79. Cisco UCS validated 7.2.1.2.80. Common Criteria EAL 4+ 7.2.1.2.81. EMC VSPE X validated 7.2.1.2.82. NetApp FlexPod validated

7.2.1.2.83. VCE Vblock validated 7.2.1.2.84. **Antimalware**

7.2.1.2.85. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
7.2.1.2.86. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
7.2.1.2.87. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção;
7.2.1.2.88. A mesma solução deverá ter a capacidade de realizar o rastreamento de códigos maliciosos em tempo real, por demanda e agendado em ambiente VMware sem a necessidade de agentes nas máquinas virtuais.
7.2.1.2.89. A solução deverá ter a capacidade de impedir a gravação de malwares realtime em ambiente VMware 4.1 ou superior com Vshield Endpoint sem ter agente instalado nos guests Vms.
7.2.1.2.90. A solução deve permitir proteção de antimalware em ambientes Linux (Ubuntu,CentOS, Red Hat e SuSe) utilizando agentes.
7.2.1.2.91. A solução deverá permitir a proteção de antimalware em ambientes Windows com e sem agentes.
7.2.1.2.92. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autotizadas.
7.2.1.2.93. A solução deverá oferecer scanear processos em memória em busca de Malware.
7.2.1.2.94. O scan de arquivos comprimidos deverá ser de no minimo 6 camadas de compressão;
7.2.1.2.95. O scan de arquivos comprimodos do tipo OLE deverá ser de no minimo 20 camadas de compressão;
7.2.1.2.96. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta.
7.2.1.2.97. A solução deverá mostrar informação de data sobre o ultimo scan agendado ou manual executado.
7.2.1.2.98. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware.

7.2.1.2.99. Inspeção de Pacotes (HIPS/Virtual Patching)

7.2.1.2.100. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

7.2.1.2.101. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
7.2.1.2.102. A solução deverá conter regras pré-definidas para detecções de ransonware para as principais famílias deste tipo de malware;

7.2.1.2.103. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão. A opção de detecção e bloqueio deverá possibilitar ser implementada de forma global (todas as regras) e apenas para uma regra ou grupos de regras;
7.2.1.2.104. Precisa conter regras de defesa para blindagem de vulnerabilidades eataques que explorem os seguintes sistemas operacionais: Windows 2000, 2003, 2008, Linux Red Hat, Suse, CentOS, Solaris além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache.
7.2.1.2.105. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
7.2.1.2.106. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
7.2.1.2.107. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;
7.2.1.2.108. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;
7.2.1.2.109. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
7.2.1.2.110. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;
7.2.1.2.111. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
7.2.1.2.112. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;
7.2.1.2.113. Deverá ser capaz de inspecionar tráfego incoming SSL;
7.2.1.2.114. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: Sql injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;
7.2.1.2.115. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
7.2.1.2.116. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
7.2.1.2.117. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
7.2.1.2.118. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
7.2.1.2.119. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a

capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
7.2.1.2.120. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito; 7.2.1.2.121.As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar; 7.2.1.2.122.As regras de IPS de vulnerabilidade deverão apresentar severidade baseada
em CVES;
7.2.1.2.123.As regras de IPS poderão ter sua capacidade de LOG desabilitado; 7.2.1.2.124.As regras de IPS quando disparadas poderão ter a possibilidade de emitir um
alerta;
7.2.1.2.125.As regras devem ser atualizadas automaticamente pelo fabricante; 7.2.1.2.126.Poderá atuar no modo em linha para proteção contra ataques ou modo escuta
para monitoração e alertas;
7.2.1.2.127.Devem ser fornecidas 25 licenças da solução para proteção dos servidores (físicos e/ou virtuais) para a excelência da prestação do serviço.

7.2.1.3. Soluções de Segurança para Estações de Trabalho

7.2.1.3.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

7.2.1.3.1.1. Windows 7 (x86/x64);
7.2.1.3.1.2. Windows 8.1 (x86/x64);
7.2.1.3.1.3. Windows 10 (x86/x64);

7.2.1.3.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

7.2.1.3.3. Deve ser integrada ao Windows Security center, quando utilizado plataforma Microsoft;
7.2.1.3.4. Deve possuir capacidade nativa de integração com modulo da análise virtual para ameaças desconhecidas com suporte a sandbox do mesmo fabricante da solução ofertada
7.2.1.3.5. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de Tróia, key loggers, programas de propaganda, rootkits, phishing, dentre outros;
7.2.1.3.6. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em:
7.2.1.3.7. Processos em execução em memória principal (RAM);
7.2.1.3.8. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
7.2.1.3.9. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip e exe;
7.2.1.3.10. Arquivos recebidos por meio de programas de comunicação instantânea (msn messenger, yahoo messenger, google talk, icq, dentre outros).
7.2.1.3.11. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em

linguagens tais como javascript, vbscript/Activex;

7.2.1.3.12. Deve possuir detecção heurística de vírus desconhecidos;

7.2.1.3.13. Deve permitir configurar o consumo de cpu que será utilizada para uma varredura manual ou agendada;

7.2.1.3.14. Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

7.2.1.3.15. Em tempo real de arquivos acessados pelo usuário;

7.2.1.3.16. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita dearquivo;

7.2.1.3.17. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

7.2.1.3.18. Automáticos do sistema com as seguintes opções:

7.2.1.3.19. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

7.2.1.3.20. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

7.2.1.3.21. Frequência: horária, diária, semanal e mensal;

7.2.1.3.22. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados;

7.2.1.3.23. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

7.2.1.3.24. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

7.2.1.3.25. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

7.2.1.3.26. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

7.2.1.3.27. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independente da maneira de como a URL está sendo acessada;

7.2.1.3.28. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

7.2.1.3.29. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

7.2.1.3.30. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

7.2.1.3.31. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecçõesdos arquivos;

7.2.1.3.32. Funcionalidade de atualização

7.2.1.3.33. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

7.2.1.3.34. Deve permitir atualização incremental da lista de definições de vírus; 7.2.1.3.35.

Deve permitir a atualização automática do engines do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável; 7.2.1.3.36. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

7.2.1.3.37. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

7.2.1.3.38. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

7.2.1.3.39. O servidor da solução de anti-malware, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os agentes replicadores de atualizações e configurações, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

7.2.1.3.40. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização;

7.2.1.3.41. Funcionalidade de administração

7.2.1.3.42. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

7.2.1.3.43. Deve possibilitar instalação "silenciosa"; 7.2.1.3.44. Deve permitir o bloqueio por nome de arquivo; 7.2.1.3.45. Deve permitir o travamento de pastas e diretórios; 7.2.1.3.46. Deve permitir o travamento de compartilhamentos;

7.2.1.3.47. Deve permitir o rastreamento e bloqueio de infecções;

7.2.1.3.48. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;

7.2.1.3.49. Deve efetuar a instalação remota nas estações de trabalho, sem requerer outro software ou agente adicional, previamente instalado e sem necessidade de reiniciar a estação de trabalho;

7.2.1.3.50. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;

7.2.1.3.51. Deve permitir a desinstalação através da console de gerenciamento da solução; 7.2.1.3.52. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;

7.2.1.3.53. Deve ter a possibilidade de determinar a capacidade de armazenamento da área de quarentena;

7.2.1.3.54. Deve permitir a deleção dos arquivos quarentenados;

7.2.1.3.55. Deve permitir remoção automática de clientes inativos por determinado período de tempo;

7.2.1.3.56. Deve permitir integração com Active Directory para acesso a console de administração;

7.2.1.3.57. Identificar através da integração com o Active Directory, quais máquinas estão sem a solução de anti-malware instalada;
7.2.1.3.58. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
7.2.1.3.59. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
7.2.1.3.60. Deve permitir agrupamento automático de estações de trabalho e notebooks da console de gerenciamento baseando-se no escopo do Active Directory ou IP;
7.2.1.3.61. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;
7.2.1.3.62. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
7.2.1.3.63. Deve registrar no sistema de monitoração de eventos da console de anti- malware informações relativas ao usuário logado no sistema operacional
7.2.1.3.64. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;
7.2.1.3.65. Deve prover ao administrador informações sobre quais estações de trabalho e notebooks fazem parte do escopo de gerenciamento da console de anti- malware não realizaram o escaneamento agendado ou o escaneamento demandado pelo administrador no período determinado de dias;
7.2.1.3.66. Deve prover segurança através de SSL para as comunicações entre o servidor e a console de gerenciamento web;
7.2.1.3.67. Deve prover segurança através de SSL para as comunicações entre o servidor e os agentes de proteção;
7.2.1.3.68. Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;
7.2.1.3.69. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;
7.2.1.3.70. Deve permitir a criação de usuários locais de administração da console de anti-malware;
7.2.1.3.71. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;
7.2.1.3.72. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;
7.2.1.3.73. Deve bloquear acessos indevidos a área de administração do agente que não estejam na tabela de políticas definidas pelo administrador;
7.2.1.3.74. Deve permitir a gerência de domínios separados para usuários previamente definidos;
7.2.1.3.75. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;
7.2.1.3.76. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo,

médio e alto.
7.2.1.3.77. Devem ser fornecidas 300 licenças da solução de proteção das estações de trabalho para a excelência da prestação do serviço.

7.3. SOLUÇÃO DE GESTÃO DE CREDENCIAIS DE ACESSO

7.3.1. Características Básicas da Solução

7.3.1.1. Cada pacote de software ofertado deve ser instalado em sua última versão estável e estar coberto por contrato de suporte e atualização de versão pelo(s) fabricante(s) durante a vigência da garantia de 36 meses;
7.3.1.2. O conjunto de requisitos especificados para cada item da solução pode ser atendido por meio de composição de produtos de múltiplos fabricantes/fornecedores, desde que sejam atendidas as especificações técnicas mínimas e obrigatórias;
7.3.1.3. Todos os componentes constantes da Solução deverão possuir EOL (End-of-life) e EOS (End-of-support) não definidos ou anunciados para um prazo superior a 60 meses.

7.3.2. Solução de Segurança para Sistemas Críticos – Análise Comportamental e Resposta a Ações de Risco

7.3.2.1. Um dispositivo alvo da solução é definido como um servidor, uma estação de trabalho, um ativo de rede e de segurança, dentre outros mencionados a seguir, cujas credenciais de acesso passem a ser gerenciadas pela solução.

7.3.2.2. Um usuário da solução é definido como qualquer pessoa que acesse um dispositivo alvo mediante logon na solução e uso de credenciais por ela gerenciadas.

7.3.2.3. A Solução deverá prover análise comportamental, auditoria e segurança de acessos a sistemas críticos por meio de credenciais administrativas para, no mínimo, 200 dispositivos (desktops, servidores físicos e virtuais, ativos de infraestrutura – como controladores de domínio, access points/controladores WiFi, switches LAN/SAN, roteadores, appliances de segurança, roteadores, câmeras de vigilância e sistemas tecnológicos diversos) e, no mínimo 10 usuários simultâneos com acessos a sistemas críticos;

7.3.2.4. Requisitos Mínimos

7.3.2.5. Gerenciar em dispositivos-alvo baseados, em, no mínimo, as seguintes tecnologias:
7.3.2.5.1.1. Sistemas operacionais:Linux/Unix, Microsoft Windows;

7.3.2.5.2. Hypervisors:

7.3.2.5.3. VMWare, RedHat KVM e Microsoft Hyper-V;

7.3.2.5.4. Contas de usuários de sistemas;
7.3.2.5.5. Contas de usuários de serviço;

7.3.2.5.6. Credenciais do Microsoft COM+;
7.3.2.5.7. Credenciais do Microsoft Internet Information Service – IIS;
7.3.2.5.8. Credenciais do Apache TomCat;
7.3.2.5.9. Credenciais do RedHat JBoss;
7.3.2.5.10. Objetos do Microsoft Active Directory (usuários, grupos e computadores);
7.3.2.5.11. Objetos do Lightweight Directory Access Protocol – LDAP (usuários, grupos e computadores);
7.3.2.5.12. Contas de usuários e administradores de bancos de dados Microsoft SQL Server, Oracle, PostgreSQL;
7.3.2.5.13. Contas de equipamentos ativos de conectividade de redes LAN (Local Area Network) e WAN (Wide Area Network) – switches, roteadores, controladores/APs WiFi;
7.3.2.5.14. Contas de equipamentos ativos de conectividade de redes SAN (Storage Area Network) e NAS (Network Attached Storage);
7.3.2.5.15. Contas de usuários e administradores de consoles de gerenciamento de computadores servidores;
7.3.2.5.16. Contas de usuários e administradores de estações de trabalho; 7.3.2.5.17. Contas de equipamentos dedicados à segurança, tais como Firewall, IPS,
AntiSpam e filtros de conteúdo;
7.3.2.5.18. Contas de equipamentos dedicados à segurança física, tais como câmeras de vigilância, catracas, etc;
7.3.2.5.19. Credenciais de nuvem em VMWare ESXi, Azure, Office 365.

7.3.2.6. A solução deve possuir função de monitoramento e análise de comportamento, que toma por base os eventos gerados por todos ítens desta especificação técnica;
7.3.2.7. Deve montar perfis de comportamento dos usuários acessando todos os dispositivos-alvo através da solução, por meio dos eventos coletados;
7.3.2.8. Deve alertar abusos e comportamentos fora dos padrões aprendidos/mapeados;
7.3.2.9. Exibir de forma gráfica o resumo dos eventos recebidos pela plataforma, classificados por origem, tais como LDAP, SIEM e a própria solução;
7.3.2.10. Deve detectar os seguintes comportamentos anormais:

7.3.2.10.1. Acesso privilegiado a solução durante horários irregulares, quando um usuário recupera uma senha de conta privilegiada em uma hora irregular de acordo com seu perfil comportamental;
7.3.2.10.2. Acesso privilegiado a solução durante dias irregulares, quando um usuário recupera uma senha de conta privilegiada em um dia irregular de acordo com seu perfil comportamental;
7.3.2.10.3. Acesso excessivo a contas privilegiadas, quando um usuário acessa contas privilegiadas com mais frequência do que o normal, de acordo com seu perfil comportamental;

7.3.2.10.4. Acesso privilegiado a solução através de IP irregular ou desconhecido, quando um usuário acessa contas privilegiadas de um endereço IP ou sub-rede incomum, de acordo com seu perfil comportamental;
7.3.2.10.5. Acesso privilegiado não gerenciado, quando uma conexão com uma máquina é feita com uma conta privilegiada que não é gerenciada na solução;
7.3.2.10.6. Máquina acessada a partir de endereços IP incomuns;
7.3.2.10.7. Máquina acessada durante horários irregulares, quando uma máquina é acessada em um horário irregular, de acordo com seu padrão de utilização;
7.3.2.10.8. Acessos excessivos a uma máquina;
7.3.2.10.9. Acesso anômalo a várias máquinas, quando uma conta efetuou login em um grande número de máquinas inesperadas durante um tempo relativamente curto;
7.3.2.10.10. Máquina incomum originando acesso;
7.3.2.10.11. Usuário incomum logando de uma máquina de origem conhecida; 7.3.2.10.12.Suspeita de roubo de credenciais, quando um usuário se conecta a uma máquina sem primeiro recuperar as credenciais necessárias da solução; 7.3.2.10.13.Alteração de senha suspeita, quando é identificada uma solicitação para alterar
ou redefinir uma senha ignorando a solução;
7.3.2.10.14.Acesso privilegiado realizado fora da solução, diretamente no dispositivo alvo; 7.3.2.10.15.Usuário inativo da solução, quando ocorrem indicações de atividade de um
usuário inativo;
7.3.2.10.16. Delegação não restrita, através da análise das contas de domínio, que recebem privilégios de delegação permissivos e, portanto, expõem o domínio a um alto risco;
7.3.2.10.17. Contas SPN vulneráveis, quando as contas privilegiadas com configuração de SPN (nome principal de serviço) podem estar vulneráveis a ataques de força bruta e de dicionário off-line, permitindo que um usuário interno malicioso recupere a senha de texto sem criptografia da conta;
7.3.2.10.18. Atividades suspeitas detectadas durante uma sessão privilegiada, quando é identificada uma sessão privilegiada com atividades (comandos e anomalias na solução) definidas como suspeitas;
7.3.2.10.19. Conta de serviço conectada interativamente, quando a solução identifica um logon interativo realizado por uma conta de serviço;
7.3.2.10.20. Credenciais expostas, quando os serviços que se conectam ao LDAP expõem credenciais de contas em texto não criptografado.

7.3.2.11. Realizar a identificação e o correlacionamento de todos eventos citados combinando as ações mencionadas que caracterizam comportamentos anormais como, por exemplo, usuário acessando a solução em horário e máquina incomuns, com acesso originado de IP incomum, utilizando conta não anteriormente utilizada (suspeita de roubo de credencial);
7.3.2.12. Permitir a classificação de eventos por níveis de risco e respostas automáticas (suspensão e terminação de sessões) baseadas nos mesmos;
7.3.2.13. Possibilitar colocar sessões em quarentena, pendentes de liberação e terminação pelo administrador;
7.3.2.14. Permitir o encerramento automatizado da sessão em caso de detecção de atividade suspeita de alta criticidade/risco;
7.3.2.15. Permitir que soluções de terceiros também possam encerrar sessões suspeitas (ex: SIEM/UEBA executa a terminação de sessão);

7.3.2.16. Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em Comandos Linux, Comandos, janelas e aplicações Windows, Expressões regulares para comandos em geral e Eventos configurados manualmente, permitindo a atribuição de nível de risco customizado;
7.3.2.17. Monitorar e avaliar as atividades de contas ou grupos privilegiados que não são administrados pela solução;
7.3.2.18. Proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade de senha que incluem, no mínimo, o comprimento da senha (quantidade de caracteres), a frequência de troca da senha, a especificação de caracteres permitidos ou proibidos na composição da senha e o gerenciamento do histórico das senhas geridas;
7.3.2.19. Mitigar problemas de segurança relacionados ao compartilhamento indevido de credenciais privilegiadas que são armazenadas localmente em dispositivos e também de contas que não são gerenciadas de forma centralizada por serviços de diretórios;
7.3.2.20. Descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados. Além disso, a solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas;
7.3.2.21. Gerenciar, de forma segura, senhas utilizadas por contas de serviço, evitando a utilização de senhas em texto claro por scripts ou rotinas dos equipamentos;
7.3.2.22. Garantir a implementação dos privilégios mínimos necessários, provendo acesso às senhas das contas privilegiadas somente ao pessoal autorizado;
7.3.2.23. Garantir a quantidade de acessos à sua interface conforme a necessidade do CONTRATANTE, podendo inclusive serem ilimitados. Não é aceita a limitação do número de contas que podem ser gerenciadas em um alvo licenciado;
7.3.2.24. Deve utilizar banco de dados, para armazenamento de credenciais, com as melhores práticas de segurança, com mecanismo de blindagem do sistema operacional através da desativação ou desinstalação de serviços e portas de acesso não essenciais ao funcionamento da solução;

7.3.2.24.1. Caso o banco de dados utilizado para armazenamento de credenciais seja de terceiros, a solução deverá ser entregue com licenças de software que o compatibilize com a solução;
7.3.2.24.2. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação;

7.3.2.25. Utilizar banco de dados para armazenamento de credenciais que permita alta disponibilidade e mecanismos para a recuperação de desastres, e que também seja compatível com soluções de backup e arquivamento disponíveis no mercado;
7.3.2.26. Permitir o Backup e Recovery de seu Banco de Dados, bem como das Configurações de Software estabelecidas, permitindo a execução de Backups automatizados, com a programação/agendamento de horários;
7.3.2.27. Suportar a implementação em parque computacional Windows Server 2012 R2 e Windows Server 2016;
7.3.2.28. Suportar instalação em VMWare ou Hyper-V;

7.3.2.28.1. Caso não seja compatível, a solução deverá ser entregue com hardware e licenças de software (ex.:hypervisor diverso ao do item acima ou sistema

operacional específico) que a compatibilize com as ferramentas de infraestrutura do CONTRATANTE;

7.3.2.28.2. Para o caso acima, a empresa contratada deverá prestar suporte também dos componentes adicionais a serem entregues, diretamente ou por subcontratação;

7.3.2.29. Prover, sem custos adicionais para a CONTRATANTE, alta disponibilidade dos elementos críticos da solução com funcionamento em modo ativo-ativo em cada uma das localidades (site principal e site redundante adicional), com chaveamento entre localidades (sites), garantindo que o processo seja transparente aos usuários conectados e a normalização das funcionalidades ocorra em até 5 (cinco) minutos, caso exista perda de comunicação;

7.3.2.30. Caso seja necessário, a CONTRATANTE proverá a infraestrutura (servidores/software em ambiente virtualizado, S.O., camada de balanceamento/redirecionamento de tráfego, etc) para implantação e uso da solução em alta disponibilidade;

7.3.2.31. Prover, no mínimo, um ambiente adicional externo da solução em produção para testes e homologação, replicando as mesmas licenças e funcionalidades do ambiente de produção;

7.3.2.32. A CONTRATANTE atualmente dispõe de licenças CAL (Client Access License) do serviço Microsoft Remote Desktop Services (RDS) para acessos RDP aos serviços Windows, que poderão ser utilizadas caso a solução fornecida utilize estas funcionalidades, para garantir a continuidade da experiência dos usuários;

7.3.2.33. Ter a capacidade de gerenciar credenciais que estejam em sistemas localizados em múltiplas localidades geográficas e domínios, independentemente de sua quantidade;

7.3.2.34. Permitir a opção de implementar o gerenciamento de troca de senhas em redes segregadas e remotas a fim de acomodar links de alta latência, redes isoladas (DMZ) e outras restrições semelhantes;

7.3.2.35. Possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as credenciais gerenciadas pela mesma. Deve ainda ser compatível com os seguintes métodos e padrões de criptografia:

7.3.2.35.1. AES com chaves de 256 bits;

7.3.2.35.2. Encriptação PKCS#11 ou superior por hardware utilizando dispositivos de HSM devidamente homologados pelo(s) fabricante(s) da solução ofertados;

7.3.2.35.3. FIPS 140-2;

7.3.2.36. Incorporar medidas de segurança, incluindo:

7.3.2.36.1. Certificação Common Criteria (CC) - ISO/IEC 15408 - como garantia de segurança do método utilizado no desenvolvimento do sistema;

7.3.2.36.2. Criptografia, a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações web dos usuários finais;

7.3.2.37. Ser capaz de exportar a chave de criptografia ou credencial equivalente do local de armazenamento das credenciais (repositório seguro), para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso a todas as senhas de identidades privilegiadas gerenciadas pela solução;

7.3.2.38. Integrar-se com soluções de autenticação de duplo fator, incluindo tokens físicos, tokens em software, tokens de evento, tokens de tempo e outras que possuam suporte para envio de

tokens via SMS e email;
7.3.2.39. Prover uma interface gráfica para que os administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem necessidade de serviços profissionais de terceiros;
7.3.2.40. Prover arquitetura para que os administradores possam configurar as integrações que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros;

7.3.2.40.1. A funcionalidade deve permitir que o administrador configure a comunicação com aplicações de terceiros utilizando scripts, macros, chamadas executáveis, linguagens de programação diversas e aceite protocolos variados incluindo,no mínimo, WMI, SSH e HTTP/HTTPS;

7.3.2.41. Integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas, das seguintes ações:

7.3.2.41.1. Atividades administrativas de delegação e revogação de acesso as credenciais privilegiadas;
7.3.2.41.2. Atividades de recuperação, liberação e alterações de senhas; 7.3.2.41.3. Atividades executadas pelos usuários na aplicação web; 7.3.2.41.4. Eventos agendados.

7.3.2.42. Descobrir e alterar credenciais em ambiente Windows, incluindo contas nomeadas, administradores 'built-in' e convidados, para determinar movimentações laterais (pass-the-hash), exibidas em mapa de rede gráfico e interativo ou através de relatórios e interface de gerenciamento;
7.3.2.43. Descobrir e alterar credenciais privilegiadas em ambientes Linux e Unix;
7.3.2.44. Gerenciar credenciais em interfaces de gerenciamento de servidores “out-of- band”, tais como Dell iDrac, IBM IMM ou compatíveis com o padrão IPMI – Intelligent Platform Management Interface;
7.3.2.45. Descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP V3;
7.3.2.46. Descobrir e alterar contas privilegiadas usadas em serviços web em, no mínimo, aplicações baseadas em Microsoft IIS);
7.3.2.47. Descobrir e alterar processos interdependentes e credenciais de serviço, incluindo credenciais em ambientes clusterizados;
7.3.2.48. Permitir o agrupamento lógico de credenciais, obedecendo uma hierarquia, a fim de simplificar a configuração e aplicação de políticas apropriadas para diferentes tipos de sistemas alvo, além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas;

7.3.2.49. Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e realizar verificações agendadas e automáticas a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino correspondam às mesmas senhas armazenadas no banco de dados da solução. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas notificando este evento; Proteger as senhas de credenciais compartilhadas que seriam normalmente armazenadas em planilhas e arquivos em texto claro;
7.3.2.50. Conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH" sem que os usuários

vejam qualquer senha, garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso, devendo conceder acesso a:

7.3.2.50.1. Sistemas e aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução, sem que haja login interativo por parte do usuário no sistema operacional do servidor de destino, possibilitando habilitar gravação da sessão caso seja necessário. Exemplo: Executar o SQL Management Studio com credencial de SA (System Administrator) sem que o usuário conheça a senha e sem necessidade de login interativo prévio do usuário no sistema operacional do host de destino;
7.3.2.50.2. Sistemas baseados em Remote Desktop e SSH sem que os usuários vejam a senha. A senha vigente no momento (estática ou dinâmica) deverá ser provida para as aplicações ou conexões remotas devendo ser recuperadas de forma automática e transparente do banco de dados da solução;
7.3.2.50.3. As sessões acessadas podem ser monitoradas ao vivo, com compartilhamento de tela e controle de periféricos, como teclado e mouse (assistência remota), e por meio de gravação de vídeos das mesmas, em formato padrão de execução não proprietário da solução, possibilitando que os vídeos gerados possam ser armazenados de modo seguro em drivers locais de rede, pastas compartilhadas, etc.;
7.3.2.50.4. Caso tenha formato proprietário, a solução deverá conter meios de acessar os vídeos.
7.3.2.50.5. Filtrar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado;
7.3.2.50.6. A função de gravação de sessões deve realizar o isolamento de sessões de acesso, atuando como um proxy/servidor de salto entre a máquina do usuário e o ativo a ser acessado;
7.3.2.50.7. A função de gravação de sessões deve ser provida em alta disponibilidade, no modelo ativo-ativo ou ativo-stand-by, tanto no site principal quanto no site adicional previsto para a função DR;
7.3.2.50.8. Quando em ambiente distribuído entre dois Data Centers, a solução deverá permitir que cada equipamento armazene suas gravações de maneira segura em storage local, evitando a transmissão desnecessária de dados entre diferentes Data Centers;
7.3.2.50.9. Ainda que as gravações estejam armazenadas em locais diferentes, a solução deve permitir que essas evidências sejam consultadas a partir de qualquer console web instalada, de maneira centralizada;

7.3.2.51. Permitir que os usuários solicitem acesso aos gestores através de interfaceweb intuitiva;
7.3.2.52. Realizar automaticamente a descoberta, detecção, importação e armazenamento no repositório seguro de chaves SSH em sistemas Linux, implementando:

7.3.2.52.1. Suporte a chaves nos tamanhos 1024, 2048, 4096 e 8192 bits;

7.3.2.52.2. Análise da relação de confiança das chaves detectadas com outras máquinas na rede;
7.3.2.52.3. Auditoria e controle dos acessos às chaves por sistema de aprovações; 7.3.2.53.4. Renovação periódica ou sob demanda das chaves;
7.3.2.53.5. Verificação da validade e sincronia das chaves com o destino; 7.3.2.53.6. Reconciliação de chaves, renovando-as e armazenando-as novamente;

7.3.2.53.7. Conexão transparente a ativos da rede,utilizando as chaves armazenadas; 7.3.2.53.8. Gerenciamento em grupos, permitindo que múltiplas máquinas herdem a
mesma chave SSH.

7.3.2.53. Permitir que os comandos executados em sistemas Linux monitorados sejam gravados em modo texto;
7.3.2.54. Possuir funcionalidade de “AD Bridge” para integração de servidores Linux/Unix no Active Directory, acompanhando a mesma nomenclatura e grupos do diretório LDAP ou AD;
7.3.2.55. Provisionar na plataforma Unix-like as contas e grupos do Active Directory que possuam permissão de acesso, de maneira automatizada e transparente;
7.3.2.56. Fornecer aplicação web para acesso às funcionalidades básicas da solução que seja compatível com ao menos dois dos principais navegadores do mercado (Internet Explorer, Google Chrome e Firefox);
7.3.2.57. Oferecer em sua aplicação web diferentes visões e opções de acordo com as permissões dos usuários, mostrando, por exemplo, apenas as funcionalidades delegadas àquele usuário;
7.3.2.58. Suportar métodos para registrar e relatar qualquer ação realizada e detectada pela solução, incluindo registros de aplicações baseadas em texto, auditoria de banco de dados, aplicações syslog, notificações de e-mail;
7.3.2.59. Permitir o envio automático de logs para servidores SYSLOG, de forma aderente ao disposto em RFC 5424 – The Syslog Protocol (IETF);
7.3.2.60. Ser configurável para enviar alertas disparados pelo sistema e eventos de usuário baseados nos arquivos de log, valores de registro, e-mail, logs de evento do Windows, Syslog, enfileiramento de mensagens Microsoft e executando aplicações específicas;
7.3.2.61. Controlar o acesso aos relatórios se baseando nas permissões configuradas na solução;
7.3.2.62. Registrar cada acesso, incluindo os acessos via aplicação web, para solicitações de senha, aprovações, checkout's, mudanças de delegação, relatórios e outras atividades. Devem ser registrados os acessos à console de gerenciamento da solução, tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas;
7.3.2.63. Caso os componentes da solução sejam segregados uns dos outros, a sua intercomunicação não deverá conter senhas em texto claro;
7.3.2.64. Criar relatórios que podem ser exportados em pelo menos um dos formatos editáveis: HTML, CSV, XLSX ou XLS;
7.3.2.65. A solução deverá disponibilizar:

7.3.2.65.1. Mecanismo de retirada e devolução de contas e senhas compartilhadas; 7.3.2.66.2. Definição de tempo de validade: permitir o estabelecimento de tempo de
validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;
7.3.2.66.3. Troca automática da senha no sistema gerenciado, após a sua devolução ou após o vencimento do tempo de validade estabelecido;
7.3.2.66.4. Troca de senhas por demanda: permitir a troca de senhas nos sistemas gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (grupo de todos os sistemas operacionais UNIX, por exemplo);

7.3.2.66. Ser capaz de, durante o processo de definição da política de composição de senha:

7.3.2.66.1. Gerar senhas aleatórias com extensão de 127 (cento e vinte e sete) caracteres ou mais;
7.3.2.66.2. Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos;
7.3.2.66.3. Especificar qual o tipo de caractere na composição das senhas a serem geradas;
7.3.2.66.4. Implementar controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada. Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de acesso a esses grupos, onde esses privilégios de acesso possam ser atribuídos por critérios como tipo de dispositivo, sistemas operacionais, banco de dados e aplicativos de virtualização;
7.3.2.66.5. Garantir que a senha gerada seja diferente do nome da conta correspondente. Exemplo: se a credencial ou conta tem o nome “Administrador” a senha gerada jamais pode ser composta da mesma forma;
7.3.2.66.6. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha;
7.3.2.66.7. Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial;
7.3.2.66.8. Garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo;

7.3.2.67. Permitir a definição de Fluxos de Aprovação (Workflows) para obtenção de acesso às Contas Privilegiadas, com as seguintes características:

7.3.2.67.1. Personalização de fluxos: permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta, e aprovação de, pelo menos, um responsável;
7.3.2.67.2. Permitir a aprovação perante um agendamento de ações administrativas; ou seja; a aprovação do acesso ocorrerá em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos;
7.3.2.67.3. No que diz respeito à descoberta automatizada de identidades privilegiadas, a solução deve ser capaz de encontrar contas de usuários privilegiados que possam ser gerenciadas pela solução, permitindo ou não que a conta descoberta seja gerenciada pela solução;
7.3.2.67.4. Ser capaz de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço em todos os locais onde estejam sendo utilizadas;
A descoberta automática deve ser realizada por buscas no Active Directory (AD) e por intervalos de endereços IP; Suportar, através da interface Web para acesso e recuperação das senhas, de forma nativa, a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução;
7.3.2.68. A interface web e de administração deverão ser compatíveis com os seguintes métodos de autenticação de duplo fator: certificados digitais, smart cards, tokens RSA, Oauth ou Google Authentication, para todos os usuários da solução;
7.3.2.69. A solução deve fornecer dados ad-hoc agendados, relatórios em tempo real dos usuários, contas, configuração da solução e informações sobre os processos da solução;
7.3.2.70. A solução deve apresentar relatórios com visibilidade hierárquica, contendo listas e filtros de ordenação, de tal forma que os usuários possam detalhar as informações e os recursos que desejam acessar;
7.3.2.71. A solução deve fornecer relatórios de auditoria que disponibilizem detalhes das

interações dos usuários com a solução, tais como:

7.3.2.71.1. Auditoria detalhada, com no mínimo, atividade de login e logoff dosusuários; 7.3.2.73.2. Alterações nas funções de delegação;
7.3.2.73.3. Adições, deleções e alterações de senhas gerenciadas pela solução; 7.3.2.73.4. Operações das senhas dos usuários, incluindo check-in e check-out, solicitações negadas e permitidas;
7.3.2.73.5. Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e outros critérios;

7.3.2.72. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:

7.3.2.72.1. Lista de sistemas gerenciados; 7.3.2.74.2. Senhas armazenadas; 7.3.2.74.3. Eventos de alteração de senha; 7.3.2.74.4. Permissões de acesso web;
7.3.2.74.5. Auditoria de contas, sistemas e usuários; 7.3.2.74.6. Alerta em tempo real.

7.3.3. Solução de Segurança para Sistemas Críticos – Proteção contra Tomada de Controle da Rede

7.3.3.1. Para fins de volumetria, deve ser entregue proteção para no mínimo 3 controladores de domínio AD (Active Directory);
7.3.3.2. Deve proteger o Controlador de Domínio contra roubo de identidade e acesso não autorizado;
7.3.3.3. Deve monitorar atividades internas no controlador de domínio e tráfego de segmento de rede que este esteja instalado, para confirmação de integridade das solicitações e tickets Kerberos utilizados nos equipamentos e contas de usuário;
7.3.3.4. Deve detectar em tempo real atividades anômalas, típicas de ataques ao protocolo de autenticação Kerberos, como roubo de credenciais, movimentação lateral e escalonamento de privilégios;
7.3.3.5. Deve detectar a extração e uso de um Kerberos TGT (ticket de concessão de tickets) da memória LSASS (Subsistema de autoridade de segurança local) em um host para obter acesso a outros recursos da rede (Pass-the-ticket); Deve detectar a recuperação e exploração de hashes de senha armazenados no banco de dados do SAM (Security Accounts Manager) ou do Active Directory para representar um usuário legítimo (Pass-the-Hash);
7.3.3.6. Deve detectar a obtenção de acesso ao KDC (Kerberos Key Distribution Center) para geração de token principal de segurança que fornece acesso completo a um domínio inteiro (Golden Ticket);
7.3.3.7. Deve detectar o uso do hash de uma conta de usuário para obter um tícket do Kerberos, que é usado para acessar outras contas e recursos de rede (Overpass- the-Hash);
7.3.3.8. Deve detectar a modificação das configurações de permissão de ticket do Kerberos para obtenção de acesso não autorizado aos recursos da rede PAC Manipulation (Manipulação de Certificado de Atributo de Privilégio);
7.3.3.9. Deve detectar a recuperação maliciosa de credenciais do controlador de domínio (DCSync);

8. PRAZOS DE EXECUÇÃO E DE ACEITE E NATUREZA DOS SERVIÇOS

8.1. Os serviços de que tratam os itens 1 a 4 referem-se à prestação de serviços mensais, de natureza contínua, razão pela qual podem vigorar pelo período de até 60 meses, tendo como fundamento o que dispõe o inc. II, art. 57 da Lei nº 8.666/93. O período de prestação, a partir da emissão do termo de recebimento definitivo, será o estabelecido na tabela abaixo, observadas as etapas previstas de planejamento, customização de ambiente e instalação de ativos de rede, deste Termo.

Item	Descrição	Quantidade	Meses
1	Serviço de Proteção de Perímetro com Firewall Avançado de Próxima Geração	1	36
2	Serviço de Proteção das Estações de Trabalho e Servidores de Rede	1	36
3	Serviço de Gestão de Credenciais Privilegiadas	1	36

8.2. O item 4 refere-se à prestação de serviços técnicos especializados de natureza eventual, sendo demandados de acordo com as necessidades do IGEPREV, solicitados por meio de Ordem de Serviço cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços;

8.3. A partir da assinatura do contrato, correrão os seguintes prazos:

8.3.1. Reunião de início do projeto (kick-off): 10 (dez) dias corridos;
8.3.2. Entrega do Projeto Executivo: 40 (quarenta) dias corridos;

8.3.2.1. O IGEPREV se manifestará no prazo de 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;

8.3.2.2. Havendo necessidade de ajustes, a contratada terá 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo IGEPREV, a respeito da manifestação sobre o Projeto Executivo;

9. COMPROVAÇÕES – APRESENTAR COM A PROPOSTA DE PREÇOS

9.1. Os documentos exigidos neste procedimento licitatório poderão ser apresentados em original, por meio de fotocópias autenticadas por cartório competente ou servidor da administração, ou fotocópias simples (exceto cópia de FAX) acompanhadas dos originais para cotejo no ato da apresentação.

9.2. Para fins de habilitação serão exigidas as seguintes comprovações técnicas:

9.2.1. Declaração de atendimento da LICITANTE aos requisitos de Infraestrutura dos centros de operações de segurança (SOC) especificados no item 3.1 deste documento, disponibilizando o ambiente para auditoria por parte do IGEPREV;

9.2.2. Certificados em nome dos profissionais para fins de comprovação do item 3.2.5 deste termo de referência;

9.2.3. Declarações conferidas por empresas públicas ou privadas, para fins de comprovação do item 3.3.1 deste termo de referência;

9.2.4. Declaração dos fabricantes das soluções, para fins de comprovação do item 3.3.2 deste termo de referência;

10. CONDIÇÕES DE ENTREGA E IMPLANTAÇÃO DOS SERVIÇOS

10.1. O prazo para entrega dos equipamentos e sistemas que compõem o serviço pela CONTRATADA será de 60 (sessenta) dias consecutivos, contados a partir da data da assinatura do contrato;

10.2. Os equipamentos e sistemas que compõem o serviço deverão ser entregues e instalados no IGEPREV. As fases da implantação do serviço devem contemplar:

10.2.1. Planejamento: nesta etapa a CONTRATADA deverá realizar o planejamento do projeto, onde serão definidos os prazos por atividade, as pessoas, a estratégia de implantação do serviço, o plano testes, a localização dos Appliances na arquitetura da rede do IGEPREV, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Devem-se considerar as janelas de manutenção do IGEPREV, plano de rollback e o escopo definido. Os responsáveis técnicos do IGEPREV acompanham e aprovam o planejamento.

10.2.1.1. Os prazos para a implantação de cada um dos serviços, pela CONTRATADA, estão especificados na tabela abaixo. O prazo passa a ser contado a partir da data acordada entre o IGEPREV e a CONTRATADA para implantação do serviço, com aceite oficial do IGEPREV, após a data de recebimento dos equipamentos no IGEPREV:

Serviço	**Tempo Máximo de Implantação (Dias Corridos)**
Firewall Próxima Geração	30
Proteção de Estações de Trabalho e Sevidores	30
Gestão de Credenciais Privilegiadas	30

10.2.2. Implementações: após a aprovação do planejamento deverá ser iniciado o processo de implantação, levando-se em consideração a disponibilidade das equipes envolvidas, cumprimento

dos prazos pactuados e o foco principal do projeto: tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.

10.2.3. Etapa de testes: todos os controles implantados para a ativação dos serviços gerenciados de segurança deverão ser testados a cada etapa pré-definida no planejamento. Além disso, o plano de rollback deverá garantir o retorno exequível e ágil, caso ocorra alguma falha no processo de implantação dos controles necessários à prestação do serviço.

10.2.4. Homologação: Após a conclusão dos testes, a solução deverá ser formalmente homologada pelo IGEPREV, com a finalidade de iniciar a monitoração, operação dos serviços e gerenciamento do ambiente, dentro do NMS acordado.

10.2.4.1. O IGEPREV terá o prazo de 15 (quinze) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração do(s) serviços contratados, para emitir o relatório de homologação (aceite);

10.2.4.2. O(s) serviço(s) será (ão) aceito(s) se e somente se houver comprovação de que todos os requisitos técnicos especificados neste Termo de Referência tenham sido atendidos. Essa comprovação será feita mediante observação direta das características dos equipamentos, consulta à documentação técnica fornecida e verificação dos serviços de instalação e configurações, comparadas aos termos deste edital;

10.2.5. Documentação: A CONTRATADA deverá elaborar e manter atualizada documentação das atividades e de todos os processos.

11. VALOR DO SERVIÇO

11.1. A tarifação do serviço compreenderá os seguintes valores, a serem expressos em R$ (reais):

11.1.1. Assinatura Mensal, incluindo o direito de uso dos serviços, em comodato dos equipamentos, em regime 24x7x365 (vinte e quatro horas por dia, sete dias por semana, 365 dias por ano), todos os dias do ano, considerando um contrato de 36 meses; Disponibilização de um banco de horas, a ser utilizado sob demanda;

11.2. O Total geral do contrato, para 36 meses, será o valor a ser utilizado como base para os lances do pregão. Este valor será composto pela soma das mensalidades de todos os serviços considerando 36 meses e mais o valor total do banco de horas.

12. DO PAGAMENTO

12.1.1. Parcela fixa mensal pela prestação dos serviços de manutenção e suporte técnico da solução, a ser paga até o décimo dia do mês subsequente da prestação do serviço, estando o

pagamento da primeira parcela condicionada após passado o primeiro mês da assinatura do contrato.

12.1.2. Nenhum pagamento será efetivado sem que representantes do IGEPREV atestem, por meio de Termo de Aceite e/ou Termo de Homologação, que o objeto contratado está integralmente sendo entregue/disponibilizado e/ou cumprido pela CONTRATADA.

12.1.3. A realização de qualquer pagamento pelo IGEPREV fica condicionada a apresentação dos seguintes documentos: CND- emitida pelo INSS, Certidão de Regularidade da Receita Federal e da PGFN, CND do FGTS expedida pela CEF; prova de regularidade para com as fazendas Estadual e Municipal do domicílio da sede da CONTRATADA.

12.1.4. Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência contratual.

12.1.5. Sem prejuízo ao pagamento das multas estipuladas no contrato, o IGEPREV poderá suspender quaisquer pagamentos devidos à CONTRATADA, sem incorrer em ônus adicionais, sempre que sua área gestora do contrato constatar a ocorrência de atrasos na execução do objeto contratado, retomando-os tão logo tais atrasos sejam completamente eliminados nos termos de parecer da área gestora do contrato.

12.1.6. Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário, e órgãos administrativos, atribuídos ao IGEPREV, oriunda de problemas na execução do contrato por parte da CONTRATADA, serão repassadas a esta e deduzidas do pagamento realizado pelo IGEPREV, independente de comunicação ou interpelação judicial ou extrajudicial.

13. No preço apresentado pela CONTRATADA já estão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o contrato, assim como contribuições previdenciárias, fiscais e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho, e outros, ficando excluída qualquer solidariedade do IGEPREV, por eventuais autuações.
PENALIDADES

13.1. Em caso da não implementação dos serviços no prazo previsto, sem justificativas aceitas pelo IGEPREV, serão aplicadas as seguintes penalidades:

13.1.1. Desconto de 0,25% (zero vírgula vinte e cinco por cento) do valor global do contrato, por dia de atraso na conclusão da implantação da solução;

13.1.1.1. Após o 30º (trigésimo) dia de atraso, e a critério do IGEPREV, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

13.1.2. Multa de 10% do valor global do contrato, no caso de inexecução parcial da obrigação, sem prejuízo de aplicação de outras penalidades;

13.1.3. Multa de 15% do valor global do contrato, no caso de inexecução total da obrigação, sem prejuízo de aplicação de outras penalidades;

13.1.4. Multa de 30% do valor global do contrato, no caso de rescisão por culpa da contratada, sem prejuízo de aplicação de outras penalidades;

13.2. Caso o percentual de atendimento seja inferior a 95% por três meses consecutivos do NMS especificado, será aplicada multa no valor de 1% (um por cento) do valor global do contrato.

14. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

14.1. Assegurar-se que o local de instalação dos equipamentos necessários à prestação dos serviços possui as condições técnicas e ambientas necessárias ao funcionamento dos equipamentos necessários aos serviços;

14.2. Manter Centros de Operação de Segurança (SOC) próprios para monitoramento remoto 24x7x365, com infraestrutura estritamente de acordo com as especificações deste documento;

14.3. Implantar todos os softwares e hardwares necessários à prestação dos serviços de monitoração, gerência e administração remota da segurança, conforme as especificações técnicas constantes deste Termo de Referência;

14.4. A CONTRATADA será responsável pela manutenção preventiva e corretiva dos hardwares e softwares por ela ofertados;

14.5. Todas as soluções de hardware e Software, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de comodato;

14.6. Iniciar a prestação dos serviços dentro dos prazos estabelecidos neste Termo de Referência;

14.7. Implementar/gerenciar backup de configuração de sistemas gerenciados; Realizar qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de “patches”, etc.) mediante autorização do IGEPREV;

14.8. Comunicar, imediatamente, a eminência ou ocorrência de incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, indisponibilização dos serviços (DoS), ataques por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade dos serviços do IGEPREV;

14.9. As implantações das soluções serão realizadas pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por analistas e técnicos do IGEPREV;

14.10. Resolver os chamados de serviço e suporte técnico conforme os tempos definidos nas tabelas de tempos de atendimento (NMS) deste Termo de Referência;

14.11. Substituir equipamentos com defeito, que cause a indisponibilidade de serviço dependente do mesmo, conforme o tempo estipulado na tabela de tempos de atendimento (NMS);

14.12. Manter os serviços contratados nos níveis de disponibilidade estabelecidos em item específico deste Termo de Referência;

14.13. A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados);

14.14. A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do IGEPREV, sem prejuízo aos serviços desta;

14.15. Quando previamente acordado entre as partes, a CONTRATADA poderá realizar serviços de monitoramento in loco com o acompanhamento de um representante do IGEPREV.

14.16. Registrar os tempos de atendimento dos chamados de suporte técnico ou chamados de serviços, mensais e anuais, indicando os chamados que foram atendidos dentro e fora do NMS estabelecido neste termo de referência;

14.17. Produzir e enviar por e-mail, mensalmente, relatórios analíticos a equipe gestora do IGEPREV, ou em 24h quando for demandado;

14.18. Participar, mensalmente, de reuniões presenciais, de ponto de controle, para apresentação dos indicadores de disponibilidade, diagnósticos dos ambientes monitorados, dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos, revisão das configurações e procedimentos implementados e melhorias a serem implementadas;

14.19. Garantir e manter total e absoluto sigilo sobre as informações manuseadas, as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis, assumindo inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do IGEPREV, praticado por seus empregados, conforme Acordo de Responsabilidade para Fornecedores, a ser assinado pela CONTRATADA no ato da assinatura do contrato.

15. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

15.1. Providenciar as condições técnicas e ambientais necessárias à implantação e funcionamento dos serviços;

15.2. Providenciar as autorizações de acesso aos técnicos da CONTRATADA, desde que devidamente agendado e os técnicos identificados, aos locais de instalação das soluções para as implantações e nos casos de manutenções;

15.3. Informar aos técnicos da CONTRATADA as necessidades de configuração dos equipamentos e serviços. Estas informações serão repassadas para a CONTRATADA através da abertura de chamados de suporte técnico. Quando necessário, podem ser anexados aos chamados arquivos com as necessidades de configurações;

15.4. Cumprir pontualmente todos os seus compromissos financeiros para com a CONTRATADA;

15.5. Proporcionar todas as facilidades para que a CONTRATADA possa executar os serviços de que trata este Termo de Referência, dentro das normas e condições estabelecidas em contrato;

15.6. Comunicar à CONTRATADA todas as possíveis irregularidades detectadas na execução dos serviços contratados, para a pronta correção das irregularidades apontadas;

15.7. Fiscalizar diretamente a execução dos serviços de que trata o objeto deste Termo de Referência, atestando a sua prestação se, e somente se, os serviços executados atenderem plenamente às especificações constantes deste Termo de Referência.

15.8. Rejeitar, no todo ou em parte, a solução entregue pela CONTRATADA fora das especificações deste Termo de Referência.

15.9. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados ao IGEPREV ou a terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos.

ANEXO II
MODELO DA PROPOSTA DE PREÇO

Ref.: Pregão Eletrônico nº XXXXXX-IGEPREV

Ao
INSTITUTO DE GESTÃO PREVIDENCIARIA DO ESTADO DO PARÁ – IGEPREV
Av. Alcindo Cacela nº 1962 – Bairro Nazaré – Belém (PA)
CEP: 66.0040-020 – Fone: (91) 31823506

1 OBJETO DA PROPOSTA:

1.1 Serviços de Atividade de Execução Continuada à prestação de Serviço Gerenciados de Segurança Lógica através de uma Solução Integrada composta por serviços complementares como suporte técnico e monitoração preventiva, dentre outros, e a alocação de hardware(s) e/ou software(s) necessários para a execução do serviço.

ITEM	DESCRIÇÃO	QTD	VALOR MENSAL/HORA	VALOR TOTAL (36 MESES)
01	Serviço de Proteção de Perímetro com Firewall Avançado de Próxima Geração	36	R$ XXX	R$XXX
02	Serviços de Proteção das Estações de Trabalho e Servidores de Rede	36	R$XXX	R$XXX
03	Serviço de Gestão de Credenciais Privilegiadas	36	R$XXX	R$XXX
04	Serviços Técnicos Especializados	4.000	R$XXX	R$XXX
TOTAL				**R$XXX**

1.2 PREÇO GLOBAL: R$ xxx (xxxx);

Nos preços aqui propostos estão incluídos, além dos serviços todos os materiais e equipamentos necessários a execução dos mesmos e todos os custos, benefícios, encargos, tributos, taxas e contribuições.

2 - DADOS BANCARIOS
- Banco: xxx
- Agencia: xxx
- Conta Corrente: xxxxx

3- VALIDADE: Esta proposta tem validade de 60 (sessenta) dias, contados a partir de sua apresentação

OBS: Esta proposta deverá ser em papel timbrado, assinada e datada pelo licitante. informar nº telefones fixo, celular e-mail.

Assinatura do responsável

ANEXO III

DECLARAÇÃO QUE EMPREGA 5% DE DEFICIENTE

Ref.: Pregão Eletrônico IGEPREV nº XXX/2020.

(Nome da Empresa) ----------, CNPJ N° ----------, estabelecida a ----------(endereço completo), por intermédio de seu representante legal, o (a) Sr. (a) ----------, portador (a) da Carteira de Identidade n°. ---------- e do CPF n°. ----------, DECLARA, para fim do disposto no inciso I do Art. 27 da Lei n° 8.666 de 21 de junho de 1993, que possui em seu quadro de pessoal, 5% (cinco por cento) de pessoas com deficiência em atendimento ao disposto no § 6° do Art. 28 da Constituição do Estado do Pará.

Cidade (UF), _____ de _____ de 2020.

Assinatura/carimbo

ANEXO IV

DECLARAÇÃO DE CUMPRIMENTO DAS NORMAS TRABALHISTAS, DE PROTEÇÃO AO MEIO AMBIENTE E AOS DIREITOS DA MULHER.

Ao Sr. Pregoeiro do Instituto de Gestão Previdenciária do Estado do Pará

Referente: Pregão Eletrônico n° XX/2020-IGEPREV

(Nome da Empresa), CNPJ nº, estabelecida à (endereço completo), por intermédio de seu representante legal, o (a) Sr.(a)..., portador (a) da Carteira de Identidade nº...e do CPF nº..., DECLARA, para fins de disposto no artigo 28, §4º da Constituição do Estado do Pará, que cumpre as normas trabalhistas, bem como, as do meio ambiente e de proteção aos direitos da mulher.

Belém, ... de ..... de 2020.

_____
(Assinatura)
(Firma licitante/CNPJ)
(Nome completo do declarante)

ANEXO V
MINUTA DE CONTRATO

CONTRATO ADMINISTRATIVO Nº XX/2020 – IGEPREV
PREGÃO ELETRÔNICO Nº XX/2020
PROCESSO: 2020/568274

MINUTA DE CONTRATO DE PRESTAÇÃO DE SERVIÇO DE SEGURANÇA LÓGICA ATRAVÉS DE SOLUÇÃO INTEGRADA QUE ENTRE SI CELEBRAM O INSTITUTO DE GESTÃO PREVIDENCIÁRIA DO ESTADO DO PARÁ – IGEPREV E A EMPRESA XXXXXXXXXXXXXXXXX.

O **INSTITUTO DE GESTÃO PREVIDENCIÁRIA DO ESTADO DO PARÁ**, Autarquia Estadual, criada pela Lei Complementar nº 039, de 09 de janeiro de 2002, publicado no Diário Oficial do Estado de nº 29.631, de 05 de fevereiro de 2002, pessoa jurídica de direito público, com sede na Avenida Alcindo Cacela, nº 1962 – Bairro Nazaré, CEP: 66.040-020, inscrito no CNPJ/MF sob o nº 05.873.910/0001-00, endereço eletrônico contratos@igeprev.pa.gov.br, nesta cidade, doravante denominada **CONTRATANTE**, representado neste ato por seu Presidente, **DR. ILTON GIUSSEPP STIVAL MENDES DA ROCHA LOPES DA SILVA**, brasileiro, casado, advogado, portador da carteira de identidade Nº 3159382 PC/PA, CPF: 647.085.272-68, conforme Decreto publicado no DOE Nº 34.267 de 30/06/2020 e por seu Diretor de Administração e Finanças, **FRANKLIN JOSÉ NEVES CONTENTE**, brasileiro, casado, advogado, portador da carteira de identidade Nº 3685889 PC/PA, CPF: 704.353.322-87, conforme Decreto publicado no DOE Nº 34. 276 de 09/07/2020, doravante denominada **CONTRATANTE** e de outro lado à empresa XXXXXXXXXX, com sede na Rua XXXXXXXX, XXXX Bairro XXXXX – XXXXXXX/XX, CEP XXXXXXX, inscrita no CNPJ/MF sob o nº. XXXXXXXXXXXX, neste ato representado por XXXXXXXXXX, portadora da Carteira de Identidade n° XXXXXXXX e inscrita no CPF/MF sob o n° XXXXXXXX, doravante denominada **CONTRATADA,** acordam e ajustam firmar o presente contrato de prestação de serviços, em conformidade com a legislação vigente mediante as cláusulas e condições seguintes, que reciprocamente aceitam e se obrigam a cumprir.

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O presente Contrato tem por objeto a Prestação de Serviços de Atividade de Execução Continuada referentes à prestação de Serviço Gerenciados de Segurança Lógica através de uma Solução Integrada composta por serviços complementares, como suporte técnico e monitoração preventiva, dentre outros, e a alocação de hardware(s) e/ou software(s) necessários para a execução do serviço.

1.2. Mais detalhes sobre o objeto deste contrato constam no Termo de Referência.

CLÁUSULA SEGUNDA – DA LEGISLAÇÃO APLICÁVEL

O presente Contrato está em consonância com o Edital do Pregão Eletrônico n° XX/2020; proposta apresentada; Decreto Estadual nº 534, de 04 de fevereiro de 2020, Lei Federal nº 8.666, de 21 de junho de 1993, e demais legislações correlatas.

CLÁUSULA TERCEIRA – DA APROVAÇÃO DA MINUTA

A minuta deste Contrato foi aprovada pela Procuradoria Jurídica da CONTRATANTE, conforme parecer N° 140/2020, nos termos do Parágrafo Único do art. 38, da Lei n° 8.666/1993.

CLÁUSULA QUARTA– DO REGIME DE EXECUÇÃO E DO PREÇO

4.1 A **CONTRATANTE** pagará a **CONTRADADA** pela prestação do serviço o valor de R$ XXXXX (XXXX), SOB DEMANDA, conforme valores explícitos na tabela a seguir:

ITEM	Especificação	Vigência (meses)	Unidade	Valor Unitário	Valor Total
01	Serviço de Proteção de Perímetro com Firewall Avançado de Próxima Geração	36 meses	Mês	R$ XXXX	R$ XXXX
02	Serviços de Proteção das Estações de Trabalho e Servidores de Rede			R$ XXXX	R$ XXXX
03	Serviço de Gestão de Credenciais Privilegiadas			R$ XXXX	R$ XXXX
04	Serviços Técnicos Especializados	4.000	Hora	R$ XXXX	R$ XXXX
TOTAL					**R$ XXXX**

4.2 Os itens 1, 2 e 3 serão pagos mensalmente, no valores estabelecidos. O item 4 será pago conforme utilizado, de acordo com a necessidade do Instituto, cabendo ao fiscal de contrato a sua apuração e validação prévia ao pagamento, através de ateste de nota fiscal e relatório de serviços prestados.

CLÁUSULA QUINTA- DA MANUTENÇÃO PELA CONTRATADA DAS CONDIÇÕES DE HABILITAÇÃO:

5.1 Obriga-se a **CONTRATADA** a manter, durante a vigência contratual, todas as condições demonstradas para habilitação do contrato, bem como deverá atualizar os documentos cuja validade expire durante a vigência contratual, de modo a garantir o cumprimento das obrigações assumidas.

5.2 A **CONTRATANTE** deverá ser informada sempre que houver alteração do Contrato Social da Empresa, através do envio de cópia do contrato atualizado.

CLÁUSULA SEXTA – DAS OBRIGAÇÕES DA CONTRATANTE

6.1 Providenciar as condições técnicas e ambientais necessárias à implantação e funcionamento dos serviços;

6.2 Providenciar as autorizações de acesso aos técnicos da CONTRATADA, desde que devidamente agendado e os técnicos identificados, aos locais de instalação das soluções para as implantações e nos casos de manutenções;

6.3 Informar aos técnicos da CONTRATADA as necessidades de configuração dos equipamentos e serviços. Estas informações serão repassadas para a CONTRATADA através da abertura de chamados de suporte técnico.

6.4 Quando necessário, podem ser anexados aos chamados arquivos com as necessidades de configurações;

6.5 Cumprir pontualmente todos os seus compromissos financeiros para com a CONTRATADA;

6.6 Proporcionar todas as facilidades para que a CONTRATADA possa executar os serviços de que trata o Termo de Referência, dentro das normas e condições estabelecidas em contrato;

6.7 Comunicar à CONTRATADA todas as possíveis irregularidades detectadas na execução dos serviços contratados, para a pronta correção das irregularidades apontadas;

6.8 Fiscalizar diretamente a execução dos serviços de que trata o objeto o Termo de Referência, atestando a sua prestação se, e somente se, os serviços executados atenderem plenamente às especificações constantes no Termo de Referência.

6.9 Rejeitar, no todo ou em parte, a solução entregue pela CONTRATADA fora das especificações do Termo de Referência.

6.10 A fiscalização de que trata este item não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados ao IGEPREV ou a terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos.

CLÁUSULA SÉTIMA – DAS OBRIGAÇÕES DA CONTRATADA

7.1 Assegurar-se que o local de instalação dos equipamentos necessários à prestação dos serviços possui as condições técnicas e ambientas necessárias ao funcionamento dos equipamentos necessários aos serviços;

7.2 Manter Centros de Operação de Segurança (SOC) próprios para monitoramento remoto 24x7x365, com infraestrutura estritamente de acordo com as especificações deste documento;

7.3 Implantar todos os softwares e hardwares necessários à prestação dos serviços de monitoração, gerência e administração remota da segurança, conforme as especificações técnicas constantes no Termo de Referência;

7.4 A CONTRATADA será responsável pela manutenção preventiva e corretiva dos hardwares e softwares por ela ofertados;

7.5 Todas as soluções de hardware e Software, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de comodato;

7.6 Iniciar a prestação dos serviços dentro dos prazos estabelecidos neste Contrato;

7.7 Implementar/gerenciar backup de configuração de sistemas gerenciados;

7.8 Realizar qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de “patches”, etc.) mediante autorização do IGEPREV;

7.9 Comunicar, imediatamente, a eminência ou ocorrência de incidentes de segurança: os acessos indevidos, instalação de códigos maliciosos, indisponibilização dos serviços (DoS), ataques

por força bruta, ou qualquer outra ação que vise prejudicar a funcionalidade dos serviços do IGEPREV;

7.10 As implantações das soluções serão realizadas pela CONTRATADA e todas as atividades envolvidas serão acompanhadas e coordenadas por técnicos do IGEPREV;

7.11 Resolver os chamados de serviço e suporte técnico conforme os tempos definidos nas tabelas de tempos de atendimento (NMS) no Termo de Referência;

7.12 Substituir equipamentos com defeito, que cause a indisponibilidade de serviço dependente do mesmo, conforme o tempo estipulado na tabela de tempos de atendimento (NMS);

7.13 Manter os serviços contratados nos níveis de disponibilidade estabelecidos em item específico do Termo de Referência;

7.14 A implantação das soluções, quando realizadas no ambiente de produção, poderão ter as atividades executadas após o expediente (horários noturnos ou em finais de semana e feriados);

7.15 A CONTRATADA será responsável por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do IGEPREV, sem prejuízo aos serviços desta;

7.16 Quando previamente acordado entre as partes, a CONTRATADA poderá realizar serviços de monitoramento in loco com o acompanhamento de um representante do IGEPREV;

7.17 Registrar os tempos de atendimento dos chamados de suporte técnico ou chamados de serviços, mensais e anuais, indicando os chamados que foram atendidos dentro e fora do NMS estabelecido neste termo de referência;

7.18 Produzir e enviar por e-mail, mensalmente, relatórios analíticos a equipe gestora do IGEPREV em, no máximo, 24 (vinte e quatro) horas, quando for demandado;

7.19 Participar, mensalmente, de reuniões presenciais, de ponto de controle, para apresentação dos indicadores de disponibilidade, diagnósticos dos ambientes monitorados, dirimir dúvidas sobre o serviço contratado, análise e entendimento dos relatórios gerenciais e administrativos, revisão das configurações e procedimentos implementados e melhorias a serem implementadas;

7.20 Garantir e manter total e absoluto sigilo sobre as informações manuseadas, as quais devem ser utilizadas apenas para a condução das atividades autorizadas, não podendo ter quaisquer outros usos, sob pena de rescisão contratual e medidas cíveis e penais cabíveis, assumindo inteira responsabilidade pelo uso indevido ou ilegal de informações privilegiadas do IGEPREV, praticado

por seus empregados, conforme Acordo de Responsabilidade para Fornecedores, a ser assinado pela CONTRATADA no ato da assinatura do contrato.

CLÁUSULA OITAVA - DA FISCALIZAÇÃO

8.1 O acompanhamento e a fiscalização da execução do contrato ficarão a cargo do servidor devidamente designado pela **CONTRATANTE** por meio de Portaria.

8.2 O fiscal do Contrato terá, dentre outras, as seguintes atribuições:

8.2.1 Registrar em relatório todas as ocorrências e deficiências porventura existentes e comunicar a **CONTRATADA** para a imediata correção das irregularidades apontadas, sem prejuízo das penalidades previstas neste Contrato e na lei.

8.2.2 Conferir se os serviços estão de acordo com as especificações técnicas exigidas;

8.2.3 Rejeitar no todo ou em parte os serviços prestados, se considerados em desacordo ou insuficientes, conforme os termos discriminados na proposta da **CONTRATADA**;

8.2.4 Informar ao titular da Coordenação de Tecnologia da Informação (CTIN/IGEPREV), acerca da necessidade de prorrogação do Contrato, para a tomada de providências junto à Coordenadoria de Administração e Serviços – COAS/IGEPREV.

8.2.5 Informar à Diretoria de Administração e Finanças – DAFIN/IGEPREV as ocorrências que exijam decisões e providências que ultrapassem a sua competência;

8.3 A **CONTRATANTE** exercerá a fiscalização da execução do objeto contratual, de modo a assegurar o seu efetivo cumprimento, podendo, ainda, realizar a supervisão das atividades desenvolvidas pela **CONTRATADA**, efetuando avaliação periódica.

8.4 A existência da fiscalização da **CONTRATANTE**, de nenhum modo diminui ou altera a responsabilidade da empresa contratada, na execução do Contrato.

CLÁUSULA NONA – DO PAGAMENTO

9.1 A **CONTRATADA** apresentará nota fiscal eletrônica para liquidação e pagamento da despesa pela **CONTRATANTE**, através de ordem bancária creditada em conta corrente no Banco do Estado do Pará – BANPARÁ S/A, conforme Decreto Estadual nº 877/2008, no prazo de 30

(trinta) dias, contados da apresentação da nota fiscal devidamente atestada pelo servidor designado.

9.2 No caso de devolução da nota fiscal, o prazo de pagamento estipulado no subitem 9.1 passará a ser contado a partir da data de reapresentação dos referidos documentos.

9.3 A **CONTRATANTE** poderá deduzir do montante a pagar os valores correspondentes a multas ou indenizações devidas pela **CONTRATADA**, nos termos deste Contrato.

9.4 A **CONTRATANTE** poderá, ainda, deduzir do montante a ser pago(s) valor(es) correspondente(s) às interrupções, atrasos ou não prestação de serviço, conforme dispõe o presente Contrato.

9.5 O atraso no pagamento acarretará multa moratória diária de 0,33 (zero vírgula trinta e três por cento) por dia, sobre o valor da parcela atrasada, limitado a 10% (dez por cento) do valor do contrato, mediante provocação da **CONTRATADA**, e mediante aprovação do Ordenador de Despesa da **CONTRATANTE**.

9.6 A **CONTRATANTE** efetuará os pagamentos mediante Ordem Bancária e para tanto, a **CONTRATADA** deverá informar no documento de cobrança, o nome e o número do banco, a agencia e conta corrente onde será creditado o pagamento. A Conta Corrente somente deverá estar em nome da **CONTRATADA**, de acordo com o Decreto Estadual n° 877, de 31 de março de 2008.

9.7 Parcela fixa mensal pela prestação dos serviços de manutenção e suporte técnico da solução, a ser paga até o décimo dia do mês subsequente da prestação do serviço, estando o pagamento da primeira parcela condicionada após passado o primeiro mês da assinatura do contrato.

9.8 Nenhum pagamento será efetivado sem que representantes do IGEPREV atestem, por meio de Termo de Aceite e/ou Termo de Homologação, que o objeto contratado está integralmente sendo entregue/disponibilizado e/ou cumprido pela CONTRATADA.

9.9 Nenhum pagamento será efetuado à CONTRATADA, enquanto pendente de liquidação qualquer obrigação financeira que lhe for imposta em virtude de penalidade ou inadimplência contratual.

9.10 Sem prejuízo ao pagamento das multas estipuladas no contrato, o IGEPREV poderá suspender quaisquer pagamentos devidos à CONTRATADA, sem incorrer em ônus adicionais,

sempre que sua área gestora do contrato constatar a ocorrência de atrasos na execução do objeto contratado, retomando-os tão logo tais atrasos sejam completamente eliminados nos termos de parecer da área gestora do contrato.

9.11 Todo e qualquer prejuízo ou responsabilidade, inclusive perante o Judiciário, e órgãos administrativos, atribuídos ao IGEPREV, oriunda de problemas na execução do contrato por parte da CONTRATADA, serão repassadas a esta e deduzidas do pagamento realizado pelo IGEPREV, independente de comunicação ou interpelação judicial ou extrajudicial.

9.12 No preço apresentado pela CONTRATADA já estão incluídos todos os tributos e demais encargos que incidam ou venham a incidir sobre o contrato, assim como contribuições previdenciárias, fiscais e parafiscais, PIS/PASEP, FGTS, IRRF, emolumentos, seguro de acidente de trabalho, e outros, ficando excluída qualquer solidariedade do IGEPREV, por eventuais autuações.

9.13 A realização de qualquer pagamento pelo IGEPREV fica condicionada a apresentação dos seguintes documentos: CND- emitida pelo INSS, Certidão de Regularidade da Receita Federal e da PGFN, CND do FGTS expedida pela CEF; prova de regularidade para com as fazendas Estadual e Municipal do domicílio da sede da CONTRATADA.

9.14 Será procedida consulta "ON LINE" junto ao SICAF antes de cada pagamento a ser efetuado ao fornecedor, para verificação da situação do mesmo, relativamente às condições exigidas no empenho, cujos resultados serão impressos e juntados aos autos do processo próprio.

9.15 Constatada a irregularidade fiscal e/ou trabalhista, a **CONTRATANTE** poderá aplicar, garantido o contraditório e a ampla defesa, as penalidades decorrentes do art. 87 da lei 8.666/93.

CLÁUSULA DÉCIMA – DA ATESTO DA NOTA FISCAL

Caberá ao servidor da **CONTRATANTE,** expressamente designado, atestar as notas fiscais do objeto do presente Contrato, para efeito de pagamento.

CLÁUSULA DÉCIMA PRIMEIRA – DA DOTAÇÃO ORÇAMENTÁRIA

11.1 As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria.

11.2 Os recursos orçamentários necessários para atender às despesas decorrentes deste Contrato constam do orçamento aprovado pelo IGEPREV para o exercício de 2020, como a seguir especificado:

- Unidade Orçamentária: 84201- Instituto de Gestão Previdenciária do Estado do Pará;
- Unidade Gestora: 840201 - Instituto de Gestão Previdenciária do Estado do Pará;
- Programa do PPA 2020/2023: 1508 – Governança Pública;
- Classificação Funcional Programática: 09.126.1508-8238: Gestão de Tecnologia da Informação e Comunicação;
- Fonte de Recursos: 0261000000: Recursos Diretamente Arrecadados pela Administração Indireta;
- Nº DA AÇÃO: 246021;
- Natureza de Despesa: 339040 – Serviços de Tec. da Informação e Comunicação - PJ
- Valor: R$ XXXX (XXXXX)

CLÁUSULA DÉCIMA SEGUNDA – DA ALTERAÇÃO, DO ACRÉSCIMO OU SUPRESSÃO DO CONTRATADO

12.1 No interesse da **CONTRANTE**, o valor inicial, poderá ser acrescido ou suprimido até o limite previsto no § 1º do art. 65 da Lei nº 8.666/93.

12.2 A **CONTRATADA** fica obrigada a aceitar, nas mesmas condições licitadas, os acréscimos ou supressões que se fizerem necessários.

12.3 Nenhum acréscimo ou supressão poderá exceder o limite estabelecido nesta condição, exceto as supressões resultantes de acordo entre as partes.

CLÁUSULA DÉCIMA TERCEIRA – DAS SANÇÕES ADMINISTRATIVAS

13.1 Em caso da não implementação dos serviços no prazo previsto, sem justificativas aceitas pelo IGEPREV, serão aplicadas as seguintes penalidades:

13.1.1 Multa/Desconto de 0,25% (zero vírgula vinte e cinco por cento) do valor global do contrato, por dia de atraso na conclusão da implantação da solução;

a) Após o 30º (trigésimo) dia de atraso, e a critério do IGEPREV, poderá ocorrer a não aceitação do objeto, de forma a configurar, nessa hipótese, inexecução total da obrigação assumida, sem prejuízo da rescisão unilateral da avença.

13.1.2 Multa de 10% do valor global do contrato, no caso de inexecução parcial da obrigação, sem prejuízo de aplicação de outras penalidades;

13.1.3 Multa de 15% do valor global do contrato, no caso de inexecução total da obrigação, sem prejuízo de aplicação de outras penalidades;

13.1.4 Multa de 30% do valor global do contrato, no caso de rescisão por culpa da contratada, sem prejuízo de aplicação de outras penalidades;

13.2 Caso o percentual de atendimento seja inferior a 95% por três meses consecutivos do NMS especificado, será aplicada multa no valor de 1% (um por cento) do valor global do contrato.

13.3 Ficará impedido de licitar e de contratar com a Administração e será descredenciado no Sicaf, pelo prazo de até cinco anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

13.3.1 não assinar o contrato ou a ata de registro de preços;

13.3.2 não entregar a documentação exigida no edital;

13.3.3 apresentar documentação falsa;

13.3.4 causar o atraso na execução do objeto;

13.3.5 não mantiver a proposta;

13.3.6 falhar na execução do contrato;

13.3.7 fraudar a execução do contrato;

13.3.8 comportar-se de modo inidôneo;

13.3.9 declarar informações falsas; e

13.3.10 cometer fraude fiscal.

13.3.11 Apresentar documentação falsa;

13.3.12 Ensejar o retardamento da execução do objeto;

13.3.13 Falhar na execução do contrato;

13.3.14 Fraudar na execução do contrato;

13.3.15 Comportar-se de modo inidôneo;

13.3.16 Cometer fraude fiscal;

13.4 Será deduzido do valor da multa aplicada em razão de falha na execução do contrato, o valor relativo às multas aplicadas.

13.5 A sanção de multa poderá ser aplicada a **CONTRATADA** juntamente à de impedimento de licitar e contratar estabelecida neste Termo.

13.6 O valor das multas aplicadas deverá ser recolhido no prazo de 05 (cinco) dias úteis, a contar da data da notificação. Se o valor da multa não for pago, ou depositado, será automaticamente descontado do pagamento a que a **CONTRATADA** fizer jus.

13.7 O valor da multa poderá ser descontado do pagamento a ser efetuado ao CONTRATADO.

13.8 Se o valor a ser pago a **CONTRATADA** não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual;

13.9 Se os valores do pagamento e da garantia forem insuficientes, fica a **CONTRATADA** obrigada a recolher a importância devida no prazo de 15 (quinze) dias, contado da comunicação oficial;

13.10 Esgotados os meios administrativos para cobrança do valor devido pela **CONTRATADA** à **CONTRATANTE**, este será encaminhado para inscrição em dívida ativa;

13.11 No processo de aplicação de sanções é assegurado o direito ao contraditório e à ampla defesa, facultada sempre a defesa prévia à interessada, observados os devidos prazos legais.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

A inexecução total ou parcial do Contrato enseja a sua rescisão, conforme disposto nos artigos 77 a 80 da Lei n.º 8.666/93.

CLÁUSULA DÉCIMA QUINTA – DA VIGÊNCIA

A vigência do presente Termo Contratual será de 36 (trinta e seis) meses, **contados da assinatura do Contrato**, podendo ser prorrogado nos termos da Lei, no caso de interesse das partes, mediante comunicação prévia e por escrito.

CLÁUSULA DÉCIMA SEXTA – DO REAJUSTE

16.1 O objeto deste contrato não terá seu valor alterado durante toda vigência contratual.

16.2 Após o período supra, em caso de prorrogação contratual, o reajuste terá por base o Índice Nacional de Preços ao Consumidor Amplo (IPCA).

16.3 Para os reajustes subsequentes, é necessário o interregno mínimo de 12(doze) meses, a contar dos efeitos financeiros do reajuste anterior.

16.4 Cabe a CONTRATADA solicitar o reajuste no ato da aceitação da prorrogação do contrato, caso haja, sob pena de preclusão.

CLÁUSULA DÉCIMA SÉTIMA – DA GARANTIA

17.1 A CONTRATADA deverá apresentar ao CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, contado da data de entrega do protocolo da via assinada do contrato, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor global do contrato, podendo ser efetuada por qualquer uma das seguintes modalidades:

a) Caução em dinheiro;

b) Seguro-garantia;

c) Fiança bancária;

17.2 Em se tratando de garantia prestada por intermédio de caução em dinheiro, a mesma deverá ser recolhida no Banco do Estado do Pará, em conta específica, com correção monetária, em favor do Instituto de Gestão Previdenciária do Estado do Pará, sendo que esta será devolvida atualizada monetariamente, nos termos do § 4º, do Art. 56, da Lei n.º 8.666/93;

17.3 No caso de seguro-garantia, este deverá ser feito junto a empresas de seguros e/ou resseguros autorizada a operar no mercado brasileiro pela Superintendência de Seguros Privados – SUSEP, e aceito pela CONTRATANTE, de acordo com modelo de apólice estabelecido na circular SUSEP nº 477/2013 com cobertura adicional para atendimento aos artigos 6° e 80, inciso III, da Lei 8.666/93, Circular SUSEP nº 577, de 26 de Setembro de 2018, e artigo 2° da Lei 8.987/95. Junto com a referida apólice, deverá ser apresentado documento comprobatório do ressegurador que declare a contratação do resseguro para a apólice entregue, assim como certidão de regularidade fiscal junto a SUSEP;

17.4 Caso a opção seja por utilizar título da dívida pública como garantia, este deverá conter valor de mercado correspondente ao valor garantido e ser reconhecido pelo Governo Federal, constando entre aqueles previstos em legislação específica. Além disso, deverá estar devidamente escriturado em sistema centralizado de liquidação e custódia, nos termos do Art. 61 da Lei Complementar nº 101, de 04 de maio de 2000, podendo a CONTRATANTE recusar o título ofertado, caso verifique a ausência desses requisitos;

17.5 No caso de garantia na modalidade de carta de fiança, deverá constar nesta a expressa renúncia pelo fiador, aos benefícios do art. 827 do Código Civil;

17.6 O atraso superior a 25 (vinte e cinco) dias, na apresentação da garantia, autoriza a CONTRATANTE a promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666/93;

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

17.8 Nenhum pagamento será feito a CONTRATADA até que seja aceita, pela CONTRATANTE, a Garantia de que trata esta Cláusula;

17.9 A garantia apresentada deverá alcançar 03 (três) meses após o término da vigência contratual, devendo ser renovada, tempestivamente, a cada prorrogação efetiva do Contrato, nos moldes do Art. 56 da Lei nº 8.666/93;

17.10 Se o valor da garantia for utilizado, total ou parcialmente pela CONTRATANTE, em pagamento de qualquer obrigação, inclusive indenização a terceiros, a CONTRATADA deverá proceder à respectiva reposição do valor dela no prazo de 5 (cinco) dias úteis contados da data em que for notificada pela CONTRATANTE, assim como providenciar sua complementação, em caso de acréscimo contratual, reajuste, restabelecimento de equilíbrio econômico-financeiro ou repactuação do valor contratado, nos termos do art. 65, § 1º da Lei nº 8.666/93;

17.11 A garantia somente será liberada ante a comprovação de que a CONTRATADA pagou todas as verbas rescisórias trabalhistas decorrentes da contratação. Caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia será utilizada para o pagamento destas verbas trabalhistas, diretamente pela CONTRATANTE,

17.12 A garantia assegurará qualquer que seja a modalidade escolhida o pagamento de:

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

b) Prejuízos causados à administração ou a terceiro, decorrentes de culpa ou dolo durante a execução do Contrato;

c) As multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;

d) Obrigações trabalhistas, fiscais e previdenciárias de qualquer natureza, não honradas pela CONTRATADA;

e) Prejuízos indiretos causados ao CONTRATANTE e prejuízos causados a terceiros, decorrentes de culpa ou dolo durante a execução do Contrato;

17.13 Não serão aceitas garantias nas modalidades seguro-garantia ou fiança bancária em cujos termos não constem expressamente os eventos indicados no subitem 21.12.;

17.14 À CONTRATANTE fica também autorizado a utilizar a garantia para corrigir imperfeições na execução do objeto do Contrato ou para reparar danos decorrentes da ação ou omissão da CONTRATADA, ou de seu preposto ou, ainda, para satisfazer qualquer obrigação resultante ou decorrente de suas ações ou omissões.

17.15 A autorização contida no subitem anterior é extensiva aos casos de multas aplicadas depois de esgotado o prazo recursal e aos casos de rescisão contratual com culpa da CONTRATADA, para ressarcimento da CONTRATANTE relativo a valores de multas e indenizações por venturas devidas.

17.16 Se o valor da garantia for utilizado, total ou parcialmente pela CONTRATANTE, em pagamento de multa que lhe tenha sido aplicada, a CONTRATADA deverá proceder à respectiva reposição no prazo de três dias úteis contados da data em que tiver sido notificada da imposição de tal sanção.

17.17 A CONTRATANTE não executará a garantia nas seguintes hipóteses:

a) Caso fortuito ou força maior;

b) Alteração, sem prévia anuência da seguradora ou do fiador, das obrigações contratuais;

c) Descumprimento das obrigações pela CONTRATADA decorrente de atos ou fatos da Administração ou;

d) Prática de atos ilícitos dolosos por servidores da Administração.

17.18 A garantia será considerada extinta:

a) Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Administração, mediante termo circunstanciado, de que a CONTRATADA cumpriu todas as cláusulas do Contrato e;

b) Após 03 (três) meses do término da vigência do contrato, podendo ser estendida em caso de ocorrência de sinistro.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO

O presente Contrato será publicado sob a forma de extrato no Diário Oficial do Estado do Pará, no prazo máximo de 10 (dez) dias contados da data de sua assinatura, nos termos do art. 28, § 5º da Constituição Estadual.

CLÁUSULA DÉCIMA NONA – DOS CASOS OMISSOS

O presente instrumento será regido pelas normas de Direito Público, sendo aplicado supletivamente, nos casos omissos, os princípios da teoria geral dos contratos e as disposições de direito privado, nos termos do art. 54 da Lei 8.666/93.

CLÁUSULA VIGÉSIMA – DO FORO

Fica eleito o Foro da Comarca de Belém, Estado do Pará, com renúncia expressa de qualquer outro por mais privilegiado que seja, para dirimir as dúvidas ou questões oriundas do presente contrato, não resolvidas administrativamente.

E por assim haverem ajustados, as partes assinam este contrato, em 02 (duas) vias de igual teor, na presença de 02 (duas) testemunhas abaixo, para que produza seus jurídicos e legais efeitos.

Belém (PA), XX de XXXXXXXX de 2020.

_____

ILTON GIUSSEPP STIVAL MENDES DA ROCHA LOPES DA SILVA
CONTRATANTE

_____

FRANKLIN JOSÉ NEVES CONTENTE

CONTRATANTE

_____

XXXXXXXXXXXXXX
CONTRATADA

TESTEMUNHAS

Contratada

_____
Nome/CPF:

Contratante

_____
Nome/CPF: