INSTITUTO DE DESENVOLVIMENTO DO TRABALHO - IDT

EDITAL

PREGÃO ELETRÔNICO N.º 05/2016

REGISTRO DE PREÇOS PARA FUTURA E EVENTUAL CONTRATAÇÃO DE PESSOA JURÍDICA ESPECIALIZADA PARA A PRESTAÇÃO DE SERVIÇOS GERENCIADOS DE SEGURANÇA DA INFORMAÇÃO.

Pregão Eletrônico nº 05/2016
Processo nº 2519/16

O Instituto de Desenvolvimento do Trabalho - IDT, com sede na Avenida da Universidade nº 2596, Fortaleza-CE, por intermédio da Comissão de Licitação, torna público que no dia e hora abaixo determinado, será realizada licitação para REGISTRO DE PREÇOS na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO POR LOTE que será regido pelo Decreto nº 7.892, de 23 de janeiro de 2013; Lei Federal nº 10.520, de 17 de julho de 2002; Lei Estadual Nº 15.356, de 04 de junho de 2013; Decreto Estadual Nº 28.089 de 10 de janeiro de 2006 com aplicação subsidiária da Lei nº 8.666, de 21 de junho de 1993, e respectivas alterações, além das demais disposições legais aplicáveis e do disposto no presente Edital.

1. INTRODUÇÃO

1.1. O presente Edital e seus anexos, contendo todos os documentos, dados e informações necessárias à elaboração da proposta poderão ser obtidos no endereço eletrônico www.licitacoes-e.com.br, onde se encontra o link para o Sistema de Pregão Eletrônico, no qual ocorrerá a sessão pública, realizada por meio da Internet.

1.1.1. Os interessados poderão obter maiores esclarecimentos ou dirimir suas dúvidas acerca do objeto deste Edital ou interpretação de qualquer de seus dispositivos, por escrito, até 03 (três) dias úteis anteriores à data do início da licitação, no seguinte endereço eletrônico comissao_licitacao@idt.org.br

1.2. As regras e condições do presente Pregão Eletrônico estão devidamente explicitadas neste Edital e seus anexos.

1.3. O Pregão a que se refere este Edital poderá ser adiado, revogado, por razões de interesse público, ou anulado, sem que caiba aos licitantes qualquer direito à indenização de acordo com o art. 49 da Lei Federal nº 8.666/93.

1.4. Endereço para entrega de Documentação

- ✓ Instituto de Desenvolvimento do Trabalho - IDT, Av. Da Universidade, nº 2596, Bairro Benfica, Fortaleza – Ceará, CEP. 60.020- 180.
- ✓ Horário de Funcionamento: de 08:00 às 12:00 e de 13:00 às 17:00 horas.
- ✓ Conter no anverso do envelope o nome do pregoeiro, número do pregão e o nome do órgão.

1.5. Definições. Para fins desta licitação, consideram-se:

- ✓ IDT: Instituto de Desenvolvimento do Trabalho.
- ✓ CPL: Comissão Permanente de Licitação.
- ✓ Proponente ou Licitante: a empresa que apresentar proposta nesta licitação, previamente credenciada perante o provedor do sistema eletrônico.

2. DO OBJETO

Registro de Preços para futura e eventual contratação de pessoa jurídica especializada para a Prestação de Serviços Gerenciados de Segurança da Informação, incluindo Monitoração do Ambiente Computacional e Tecnológico do SINE - IDT/CE, conforme detalhamento constante no ANEXO I - TERMO DE REFERÊNCIA.

3. DA ABERTURA

3.1. A abertura da presente licitação dar-se-á em sessão pública, por meio da INTERNET, mediante condições de segurança - criptografia e autenticação – em todas as suas fases, dirigida pelo pregoeiro designado, a ser realizada de acordo com a legislação mencionada no preâmbulo deste Edital.

3.2. INÍCIO ACOLHIMENTO DAS PROPOSTAS: **29 de junho de 2016**

3.3. DATA DE ABERTURA DAS PROPOSTAS: **13 de julho de 2016 às 14:00 horas**

3.4. INÍCIO DA SESSÃO DE DISPUTA DE PREÇOS: **13 de julho de 2016 às 14:15 horas**

3.5. REFERÊNCIA DE TEMPO: Para todas as referências de tempo contidas neste Edital será observado o **horário de Brasília/DF**.

3.6. O certame será realizado por meio do sistema do Banco do Brasil, no endereço eletrônico: www.licitacoes-e.com.br

3.7. Na hipótese de não haver expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data prevista, a sessão será remarcada, para no mínimo 48h (quarenta e oito horas) a contar da respectiva data, com divulgação no site do IDT.

4. DOS RECURSOS ORÇAMENTÁRIOS

4.1. As despesas decorrentes da Ata de Registro de Preços correrão pelas fontes de recursos das dotações orçamentárias do IDT, a ser informada quando da lavratura do instrumento contratual.

5. DAS CONDIÇÕES DE PARTICIPAÇÃO

5.1. Os interessados em participar deste certame deverão estar devidamente credenciados junto ao sistema do Banco do Brasil S.A, na página Eletrônica www.licitacoes-e.com.br.

5.2. Será garantido aos licitantes enquadrados como microempresas, empresas de pequeno porte e as cooperativas que se enquadrem nos termos do art. 34, da Lei Federal n° 11.488/2007, como critério de desempate, preferência de contratação, o previsto na Lei Complementar n° 123/2006, em seu Capítulo V – DO ACESSO AOS MERCADOS / Das Aquisições Públicas.

5.2.1. Tratando-se de microempresas, empresas de pequeno porte e cooperativas, deverão declarar no Sistema do Banco do Brasil o exercício da preferência prevista na Lei Complementar n° 123/2006.

5.3. A participação implica a aceitação integral dos termos deste edital.

5.4. É vedada a participação de pessoa física e de pessoa jurídica nos seguintes casos:

5.4.1. Sob a forma de consórcio, qualquer que seja sua constituição.

5.4.2. Que tenham em comum um ou mais sócios cotistas e/ou prepostos com procuração.

5.4.3. Que estejam em estado de insolvência civil, sob processo de falência, concordata, recuperação judicial ou extrajudicial, dissolução, fusão, cisão, incorporação e liquidação.

5.4.4. Suspensas temporariamente ou Impedidas de licitar e contratar com o Instituto de Desenvolvimento do Trabalho – IDT e/ou Administração Pública.

5.4.5. Declaradas inidôneas pelo Instituto de Desenvolvimento do Trabalho – IDT e/ou Administração Pública, enquanto perdurarem os motivos determinantes desta condição.

5.4.6. Empresas cujos dirigentes, gerentes ou sócios sejam empregados do IDT.

5.4.7. Empresa com sócio cotista que tenha parentesco até o 3º grau (consangüinidade e/ou afinidade) com algum membro da comissão de licitação e demais colaboradores direta ou indiretamente envolvidos no processo licitatório.

5.4.8. Estrangeiras não autorizadas a comercializar no país.

6. DO CREDENCIAMENTO

6.1. O credenciamento dar-se-á pela atribuição de chave de identificação e de senha, pessoal e intransferível, para acesso ao sistema eletrônico.

6.1.1. Para o credenciamento, será necessário o comparecimento do representante legal da sociedade licitante a estabelecimento indicado pelo provedor do sistema, portando cópia do contrato social, do CNPJ e dos documentos pessoais dos sócios, do Termo de Adesão ao Regulamento (de utilização do sistema), do Termo de Nomeação de Representante, que habilitará a pessoa física indicada a realizar negócios em nome da pessoa jurídica credenciada.

6.2. 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 órgão promotor da licitação a responsabilidade por eventuais danos decorrentes de uso indevido de senha, ainda que por terceiros.

6.3. A perda da senha ou a quebra do sigilo deverão ser comunicadas imediatamente ao provedor do sistema, para imediato bloqueio de acesso.

6.4. O credenciamento do licitante junto ao provedor do sistema implica na presunção de sua capacidade técnica para realização das operações inerentes ao Pregão Eletrônico.

7. DA FORMA DE APRESENTAÇÃO DA PROPOSTA ELETRÔNICA

7.1. As propostas comerciais serão recebidas exclusivamente por meio da Internet, no endereço eletrônico **www.licitacoes-e.com.br**, "Acesso Identificado", por meio da digitação da senha pessoal e intransferível do representante, observando datas, prazos, horários e demais condições estabelecidas pelo instrumento convocatório.

7.2. O encaminhamento da proposta por meio eletrônico pressupõe o pleno conhecimento e atendimento às exigências de habilitação deste Edital. O fornecedor será responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico, assumindo como firmes e verdadeiras suas propostas e lances, **vedada a identificação do proponente**.

7.3. Para simples acompanhamento da licitação, o interessado poderá acessar na internet o endereço www.licitacoes-e.com.br, onde se encontra o link para o Sistema de Pregão Eletrônico.

7.4. Os licitantes poderão retirar ou substituir as propostas por eles apresentadas, até o término do prazo para recebimento, que se inicia com a divulgação da integra do Edital no site do Sistema do Banco do Brasil, até o dia e hora previstos no item 3.2.1. deste edital.

7.5. **O campo "Informações Adicionais" poderá ser utilizado a critério do licitante**.

7.6. Ao final da disputa, a licitante que tiver ofertado **o menor preço por lote**, deverá enviar ao IDT, juntamente com os documentos de habilitação, **a proposta comercial escrita** em papel timbrado da proponente, contendo obrigatoriamente, as seguintes informações:

7.6.1. Descrição clara do(s) objeto(s) a ser (em) fornecido(s), **obedecendo ao modelo padronizado no ANEXO II.**

7.6.2. Valor unitário de cada item e valor total.

7.6.3. Valor total da proposta por extenso.

7.6.4. Validade da proposta de no mínimo **60 (sessenta) dias**, contados a partir da data de sua emissão.

7.6.5. O licitante não poderá cotar proposta com quantitativo de item/lote inferior ao determinado no edital.

7.6.6. Na cotação de preço unitário, será admitido o fracionamento do centavo somente no caso da determinação da expressão monetária de valores que necessitem da avaliação de grandezas inferiores ao centavo, sendo as frações resultantes desprezadas ao final dos cálculos.

7.6.7. **Após a apresentação da proposta não caberá desistência**.

7.6.8. Os preços propostos serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração dos mesmos, sob alegação de erro, omissão ou qualquer outro argumento não previsto em lei.

7.7. A proposta deverá considerar:

7.7.1. Que as quantidades mencionadas nos Anexos são estimadas;

7.7.2. Que o fornecimento obedecerá a conveniência e a necessidade do IDT, sem valor mínimo para faturamento e entrega;

7.7.3. Que a **vigência dos contratos** que advirão da Ata de Registro de Preços poderão ser de **até 12(doze) meses**, com possibilidade de prorrogação ou antecipação, conforme for o caso e desde que pesquisa de mercado demonstre que os preços se mantêm vantajosos, conforme Termo de Referência - ANEXO I.

7.7.4. Que a proposta apresentada e os lances formulados devem incluir todas as despesas necessárias para a perfeita execução do objeto licitado, considerando além do lucro, todos os custos e as despesas incidentes, como por exemplo: IPI, ICMS, taxas, fretes, transporte, seguros, tributos de qualquer natureza, contribuições e qualquer outra incidência fiscal e/ou tributária.

7.7.5. Que na proposta comercial deverá constar expressamente a razão social, o número do CNPJ, da CEI, Registro de ISS, endereço, número da conta corrente, agência bancária, identificação do respectivo banco, número de telefone/fax, endereço e endereço eletrônico, conforme ANEXO II.

7.8. Os preços dos serviços serão ofertados no formulário eletrônico próprio, em moeda corrente nacional e apurados à data de sua apresentação, sem inclusão de qualquer encargo financeiro ou previsão inflacionária.

7.9. O preço global da proposta comercial escrita deverá ser o mesmo ofertado por lance durante a disputa eletrônica, salvo se houver tratativas realizadas com o pregoeiro, para obtenção de preço menor.

7.10. Os preços cotados e os valores faturados, em moeda corrente nacional, serão fixos, podendo ser reajustados desde que observado o interregno mínimo de 01 (um) ano, a contar da apresentação da proposta, mediante negociações entre as partes, tendo como limite máximo a variação do IGP/DI – FGV.

7.11. Pela elaboração da proposta o proponente não terá direito a auferir qualquer vantagem, remuneração ou indenização.

7.12. A critério da Comissão de Licitação poderão ser relevados erros ou omissões formais e/ou materiais, de que não resultem prejuízo para o entendimento das propostas.

7.13. Não se admitirá proposta que apresente preço simbólico, irrisório ou de valor zero, incompatíveis com os preços de mercado, ainda que não se tenha estabelecido limite mínimo.

8. DA ABERTURA DAS PROPOSTAS E DA ACEITABILIDADE

8.1. A partir do horário previsto no item 3 (três) deste Edital terá início a sessão pública do pregão eletrônico, sendo conduzido pelo pregoeiro que cuidará do seu processamento e julgamento, podendo os licitantes a partir de então, encaminhar lances, utilizando-se exclusivamente do sistema eletrônico do Banco do Brasil.

8.1.1. Abertas as propostas, o pregoeiro fará as devidas verificações, avaliando a aceitabilidade das mesmas. Caso ocorra alguma desclassificação, será fundamentada e registrada no sistema.

8.2. Caberá ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão.

9. DA ETAPA DE LANCES

9.1. O pregoeiro dará início à etapa competitiva no horário previsto no subitem 3.4, quando, então, os licitantes devidamente conectados ao sistema, poderão encaminhar lances.

9.1.1. A cada lance ofertado o participante será imediatamente informado de seu recebimento, horário de registro e valor.

9.1.2. Os licitantes poderão oferecer lances sucessivos, observado o horário fixado e as regras de aceitação dos mesmos.

9.1.3. Só serão aceitos os lances dos licitantes cujos valores forem inferiores ao último registrado no sistema. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

9.2. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance, vedada a identificação do detentor do lance.

9.3. No caso de desconexão com o pregoeiro, no decorrer da etapa competitiva do Pregão Eletrônico, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos realizados.

9.3.1. Quando a desconexão persistir por tempo superior a dez minutos, a sessão do pregão eletrônico será suspensa e terá reinício somente após comunicação expressa aos participantes, por meio de mensagem eletrônica no chat de mensagens www.licitacoes-e.com.br, divulgando data e hora para a reabertura da sessão.

9.4. A etapa normal de lances da sessão pública será encerrada por iniciativa do pregoeiro, mediante aviso de fechamento iminente dos lances, emitido pelo sistema eletrônico aos licitantes. A partir de então transcorrerá período randômico de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema eletrônico, findo o qual estará automaticamente encerrada a recepção de lances.

9.5. O pregoeiro que detectar, na fase de lances, propostas que apresente preço global ou por lote ou unitário simbólico, irrisório ou de valor zero, incompatíveis com os preços de mercado, ainda que não se tenha estabelecido limite mínimo, poderá descartar os lances quais sejam e, a seu critério, poderá abrir procedimento administrativo para apuração de ato ilícito.

9.6. **O pregoeiro ao observar**, na fase de lances, **que algum licitante realize atos intencionais e temerários**, **que possam resultar em fracasso ou à frustração do presente certame licitatório**, ao dar lances de propostas que apresentem preço global ou por lote que frustrem a competitividade, ou seja, incompatíveis com os preços de mercado, ainda que não se tenha estabelecido limite mínimo, bem como, **algum licitante, ou um grupo de licitantes, realize(m) atos, com fins de manipular resultado, a exemplo de combinação de preços e outros similares, poderá aplicar ao(s) licitante(s) responsável(eis) sanções e penalidades previstas no Capítulo IV - DAS SANÇÕES ADMINISTRATIVAS E DA TUTELA JUDICIAL, da Lei Federal nº 8.666/93**.

9.7. O pregoeiro poderá encaminhar, pelo sistema eletrônico, contraproposta diretamente ao proponente que tenha apresentado o lance de menor preço, para que seja obtido preço melhor, e bem assim, decidir sobre sua aceitação.

9.8. O sistema informará a proposta de menor preço imediatamente após o encerramento da etapa de lances ou, quando for o caso, após negociação e decisão pelo pregoeiro acerca da aceitação do lance de menor valor.

9.9. Encerrada a etapa de lances da sessão pública, o pregoeiro determinará ao proponente, que tenha apresentado o lance de menor preço que, no prazo de **3 (três) dias úteis**, deverá entregar, na Comissão de Licitações, no endereço Av. da Universidade, 2596, Benfica Fortaleza/CE, CEP 60.020-180, a proposta comercial, endereçada ao pregoeiro, juntamente com a documentação de habilitação constantes do item 12 deste Edital.

9.10. A proposta deverá ser apresentada preferencialmente em 2(duas) vias, sendo uma original, com os preços ajustados ao menor lance, nos termos do ANEXO II – Modelo de Proposta Comercial deste Edital, com todas as folhas rubricadas e numeradas, devendo a última folha vir assinada obrigatoriamente pelo representante legal do licitante citado na documentação de habilitação, em linguagem clara e concisa, sem emendas, rasuras ou entrelinhas, com as especificações técnicas, quantitativos, marca, modelo, referência, procedência e demais informações relativas ao material ofertado.

9.10.1. O não cumprimento da entrega da documentação, dentro dos prazos acima estabelecidos acarretará na desclassificação/inabilitação, sendo convocado o licitante subsequente, e assim sucessivamente, observada a ordem de classificação.

10. AVALIAÇÃO TÉCNICA

10.1. A Comissão de Licitação encaminhará a proposta da empresa declarada vencedora aos técnicos do IDT para confirmação do atendimento das especificações solicitadas no Edital.

10.1.1. A Comissão de Licitação, caso julgue necessário, tem a prerrogativa de fazer visita às instalações próprias ou contratadas da empresa que apresentar menor preço, sendo acompanhada pelos técnicos do IDT, para confirmação do atendimento das especificações solicitadas no Edital e seus anexos.

11. DO JULGAMENTO DAS PROPOSTAS

11.1. O julgamento desta licitação será feito pelo critério de "**menor preço do lote**".

11.2. O licitante remanescente que esteja enquadrado no percentual estabelecido no art. 44, § 2º, da Lei Complementar nº 123/2006, no dia e hora designados pelo pregoeiro, será convocado na ordem de classificação, no "chat de mensagem", para ofertar novo lance inferior ao melhor lance registrado no lote, para, no prazo de 5 (cinco) minutos, utilizar-se do direito de preferência.

11.3. A Comissão de Licitação, antes de declarar o vencedor, promoverá a verificação da documentação relativa à habilitação do licitante que, na ordenação feita pelo pregoeiro, apresentou o menor preço.

11.4. Constatado o atendimento das exigências fixadas neste Edital, a licitante autora da proposta ou lance de menor valor será habilitada e declarada vencedora do certame.

11.5. Se a oferta não for aceitável, ou se a licitante classificada em primeiro lugar for inabilitada, ou na hipótese de descumprimento de qualquer outra exigência estabelecida no instrumento convocatório, caberá à Comissão de Licitação autorizar o pregoeiro a examinar a oferta subseqüente de menor preço, negociar com o seu autor, decidir sobre a sua aceitabilidade e, em caso positivo, verificar as condições de habilitação e assim sucessivamente, até a apuração de uma oferta aceitável cuja autora atenda os requisitos de habilitação, caso em que será declarada vencedora.

11.6. Declarado o licitante vencedor pela Comissão de Licitação, o pregoeiro consignará esta decisão e os eventos ocorridos em ata própria, que será disponibilizada pelo sistema eletrônico, a todos os licitantes.

11.7. Quando houver lotes com mais de um item, obrigatoriamente todos os itens do lote deverão ser cotados na proposta.

11.8. **Serão desclassificadas as propostas comerciais**:

11.8.1. Em condições ilegais, omissões, ou conflitos com as exigências deste edital.

11.8.2. Com preços superiores aos praticados no mercado, ou comprovadamente inexequíveis.

11.9. A desclassificação será sempre fundamentada e registrada no sistema.

12. DA HABILITAÇÃO

12.1. O licitante do lance de menor valor válido deverá protocolar a documentação original ou em cópia autenticada, prevista nos itens 12.2 a 12.6, e no prazo máximo de **3 (três) dias úteis**, contados do encerramento da etapa de lances da sessão pública, no endereço constante no subitem 1.4 do Edital em atenção à Comissão Permanente de Licitação do IDT, sob pena de desclassificação.

12.1.1. O licitante com sede fora do município de Fortaleza/Ceará deverá apresentar os documentos acima referidos, dentro do prazo fixado no item 12.1, usando SEDEX ou outro meio de eficiência e rapidez similares, sob pena de desclassificação.

12.1.2. **Os documentos deverão ser apresentados em original ou em cópias autenticadas**.

As publicações feitas em órgão de imprensa oficial (com a devida identificação e data), inclusive aqueles emitidos pela Internet poderão ser entregues em cópias simples.

12.1.3. As Declaração(ões) e/ou Atestado(s), que certifiquem fornecimento, emitida(s) por pessoa(s) jurídica(s) de direito privado devem estar escritas em **papel timbrado** e ter **firmas reconhecidas** de quem as emitiu.

12.2. HABILITAÇÃO JURÍDICA

12.2.1. Registro Comercial, no caso de empresa individual;

12.2.2. Ato Constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado em se tratando de sociedades comerciais e, no caso de sociedades por ações, as atas de eleição de seus diretores, regularmente registrado;

12.2.3. Inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de ata de eleição da diretoria em exercício;

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

12.2.5. Documento Oficial de Identificação e CPF do Representante da Empresa.

12.2.6. Em caso de Administração da pessoa Jurídica seja feita por procuração, a mesma deverá ser reconhecida firma e deverá ser acompanhada da documentação elencada na letra "e", do item 12.1, tanto do outorgante como do outorgado.

12.3. REGULARIDADE FISCAL E TRABALHISTA

12.3.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);

12.3.2 Prova de inscrição no Cadastro de Contribuintes Estadual ou Municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

12.3.3. Prova de Regularidade Fiscal concernente aos tributos federais e à Dívida Ativa da União, por meio de "Certidão Conjunta emitida pela Secretaria da Receita Federal do Brasil – SRFB e Procuradoria Geral da Fazenda Nacional - PGFN", dentro do prazo de validade;

12.3.4. Prova de situação regular para com a Fazenda Estadual da sede do licitante, que deverá ser feita por meio de Certidão Negativa de Débitos inscritos na Dívida Ativa Estadual;

12.3.5. Prova de situação regular para com a Fazenda Municipal da Sede do Licitante, que deverá ser feita por meio de Certidão Negativa de Débitos inscritos na Dívida Ativa Municipal;

12.3.6. Prova de situação regular perante o Fundo de Garantia por Tempo de Serviço – FGTS (art. 27, alínea "a", Lei nº 8.036, de 11/05/90), através da apresentação do CRC - Certificado da Regularidade do FGTS, emitida pela Caixa Econômica Federal;

12.3.7. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante apresentação de certidão negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei n.º 5.452, de 1º de maio de 1943, e considerando o disposto no art. 3º da Lei n.º 12.440, de 7 de julho de 2011.

12.4. QUALIFICAÇÃO ECONÔMICO-FINANCEIRA

12.4.1. Certidão Negativa de Falência ou Concordata e Recuperação Judicial expedida pelo Distribuidor Judicial, Justiça Ordinária, da sede do licitante com prazo de validade expresso na própria certidão.

12.5. QUALIFICAÇÃO TÉCNICA

12.5.1 Comprovação de aptidão para o desempenho de atividade pertinente e compatível em características com o objeto da licitação, mediante apresentação de atestado(s) fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado.

12.5.1.1 Considera-se compatível com o objeto da licitação a execução dos serviços gerenciados de segurança estritamente como descrito no item 02.01 do Termo de Referência – Anexo I.

12.6. OUTRAS COMPROVAÇÕES

12.6.1. Declaração do licitante de que não possui em seu quadro funcional nenhum trabalhador menor de dezoito anos desempenhando trabalho noturno, perigoso ou insalubre ou qualquer trabalho por menor de dezesseis anos, na forma do artigo 7.º, inciso XXXIII, da Constituição Federal, conforme o constante no ANEXO III.

12.6.2. Proposta comercial, conforme o constante no ANEXO II.

12.7. DISPOSIÇÕES GERAIS DA HABILITAÇÃO

12.7.1. Os documentos deverão estar válidos na data de entrega.

12.7.2. As certidões fiscais positivas, com efeito de negativa, serão aceitas.

12.7.3. Certidões de Dívidas/Falência e Certificados de Regularidade que não tenham prazo de validade constantes em seus textos serão consideradas válidas no presente certame licitatório por 30 (trinta) dias contados de sua expedição.

12.7.4. Não serão aceitos Declaração(ões) e/ou Atestado(s), que certifiquem fornecimento, de empresas participantes do presente certame licitatório que sejam emitidos por outra empresa, também, participante do mesmo Certame Licitatório, ou seja, **reciprocidade de Declaração(ões) e/ou Atestado(s).**

12.7.5. Havendo restrição quanto à **regularidade fiscal** da microempresa, da empresa de pequeno porte ou da cooperativa que se enquadre nos termos do art. 34, da Lei Federal nº 11.488/2007, será assegurado o prazo de 5 (cinco) dias úteis, **cujo termo inicial corresponderá ao momento em que o proponente for declarado o vencedor do certame**, para a regularização do(s) documento(s), podendo tal prazo ser prorrogado por igual período, conforme dispõe a Lei Complementar nº 123/2006 e suas alterações.

12.7.5.1. A não comprovação da regularidade fiscal, até o final do prazo estabelecido, implicará na decadência do direito, sem prejuízo das sanções cabíveis, sendo facultado ao pregoeiro convocar os licitantes remanescentes, por ordem de classificação.

12.7.6. Eventuais falhas, omissões ou outras irregularidades nos documentos de habilitação, poderão ser saneadas, inclusive mediante:

a) substituição e apresentação de documentos ou,

b) verificação efetuada por meio eletrônico hábil de informações.

12.7.7. A verificação será certificada pelo pregoeiro e deverão ser anexados aos autos os documentos passíveis de obtenção por meio eletrônico, salvo impossibilidade devidamente justificada.

12.7.8. O IDT não se responsabilizará pela eventual indisponibilidade dos meios eletrônicos, no momento da verificação. Ocorrendo essa indisponibilidade e não sendo apresentados os documentos alcançados pela verificação, a licitante será inabilitada.

12.7.9. Constatado o atendimento das exigências fixadas neste Edital, a licitante autora da proposta ou lance de menor valor será habilitada e declarada vencedora do certame.

12.7.10. A Comissão de Licitação se reserva o direito de devolver à proponente, quaisquer documentos não solicitados, independente de encadernação ou numeração de páginas.

13. DA IMPUGNAÇÃO E DOS ESCLARECIMENTOS AO EDITAL

13.1. Os pedidos de **esclarecimentos** referentes ao processo licitatório deverão ser enviados ao pregoeiro, até **3 (três) dias úteis** anteriores à data fixada para abertura das propostas, exclusivamente por meio eletrônico, no endereço comissao_licitacao@idt.org.br, informando o número deste pregão e o órgão interessado.

13.2. Até 02(dois) dias úteis antes da data fixada para a abertura das propostas, qualquer pessoa poderá **impugnar** o ato convocatório do presente Pregão, mediante **petição por escrito**, protocolada no IDT, no endereço: Avenida da Universidade, nº 2596, Bairro Benfica - CEP 60.020-180, Fortaleza–CE.

13.2.1. Não serão conhecidas as impugnações apresentadas fora do prazo legal e/ou subscritas por representante não habilitado legalmente.

13.2.2. Caberá ao pregoeiro, auxiliado pela área interessada, quando for o caso, decidir sobre a petição de impugnação no prazo de 24 (vinte e quatro) horas.

13.2.3. Acolhida a impugnação contra este edital, será designada nova data para a realização do certame, exceto se a alteração não afetar a formulação das propostas.

14. DOS RECURSOS ADMINISTRATIVOS

14.1. Após declarado o vencedor, **no prazo de até 4h úteis** e em campo próprio do sistema, qualquer licitante poderá manifestar de forma motivada a intenção de interpor recurso, quando lhe será concedido o prazo de **três dias** para apresentar o recurso com suas razões, ficando os demais licitantes, desde logo, convidados a apresentar contra-razões em igual prazo, que começará a contar do término do prazo do recorrente, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

14.1.1. Não serão conhecidos os recursos intempestivos e/ou subscritos por representante não habilitado legalmente ou não identificado no processo licitatório para responder pelo proponente.

14.1.2. As razões e contra-razões de recurso deverão ser enviadas para: Comissão Permanente de Licitação, no endereço constante no subitem 1.4., nos prazos acima definidos.

14.1.3. O licitante com sede fora do município de Fortaleza/Ceará deverá encaminhar as razões ou contra-razões, dentro do prazo fixado no item 14.1, via SEDEX ou outro meio de eficiência e rapidez similares, sob pena de decair o direito ao recurso.

14.2. A falta de manifestação imediata e motivada do licitante importará a decadência do direito de recurso e a adjudicação do objeto da licitação ao vencedor.

14.3. O acolhimento do recurso importará na invalidação apenas dos atos insuscetíveis de aproveitamento.

14.4. Os recursos serão dirigidos ao Presidente da CPL. Reconsiderando ou não sua decisão, no prazo de 5 (cinco) dias úteis, encaminhará o Pregoeiro o recurso à autoridade superior, que ratificará ou não, de forma fundamentada.

14.5. A decisão em grau de recurso será definitiva, e dela dar-se-á conhecimento aos licitantes, no endereço eletrônico constante no subitem 3.6. deste edital.

14.6. Os casos omissos ao presente Pregão Eletrônico serão solucionados pela CPL e as questões relativas ao sistema, diretamente com o Banco do Brasil.

14.7. É facultado ao IDT, em qualquer fase da licitação, promover diligência destinada a esclarecer ou complementar a instrução do processo.

15. DA ADJUDICAÇÃO E HOMOLOGAÇÂO

15.1. A adjudicação dar-se-á pelo pregoeiro quando não ocorrer interposição de recursos. Caso contrário, a adjudicação ficará a cargo da autoridade competente.

15.2. A homologação da licitação é de responsabilidade da autoridade competente e só poderá ser realizada depois da adjudicação do objeto ao vencedor.

15.3. O sistema gerará ata circunstanciada, na qual estarão registrados todos os atos do procedimento e as ocorrências relevantes.

16. DA ATA DE REGISTRO DE PREÇOS

16.1 Será registrado o preço unitário ofertado pela empresa declarada vencedora, no prazo e condições propostos, viabilizando a aquisição futura na medida das necessidades.

16.2 No decorrer da lavratura da Ata de Registro de Preços, ao preço do primeiro colocado, poderão ser registrados, se for o caso, mais 02 (dois) fornecedores, devidamente habilitados, registrando-se até o terceiro classificado, respeitada a ordem de classificação das propostas.

16.3. A vigência da Ata de Registro de Preços será de **12 (doze) meses**.

16.4. As quantidades são estimadas, não havendo obrigatoriedade por parte do IDT, em demandar a sua aquisição total, sendo que somente serão pagos os serviços efetivamente fornecidos.

16.5. O IDT poderá instaurar licitações específicas para a aquisição de serviços similares ao objeto, obedecida à legislação pertinente, sendo assegurada preferência de fornecimento ao detentor do registro, em igualdade de condições.

16.5.1. O direito de preferência de que trata o subitem anterior poderá ser exercido pelo beneficiário do registro quando, depois de realizada a licitação específica, for constatado que o preço obtido é igual ou maior que o registrado ou, após negociação, aquiescer o detentor da ata em baixar o preço registrado, igualando ou tornando-o menor que o obtido em referida licitação.

16.6. O preço registrado poderá ser revisto em decorrência de eventual redução daqueles praticados no mercado, ou de fato que eleve o custo dos bens registrados, cabendo ao IDT promover as necessárias negociações junto aos fornecedores. O detentor de preços registrados que descumprir as condições da Ata de Registro de Preços recusando-se a fornecer o objeto licitado aos participantes do SRP (Sistema de Registro de Preços), não aceitando reduzir os preços registrados quando estes se tornarem superiores aos de mercado, ou nos casos em que for declarado inidôneo ou impedido para licitar e contratar com o IDT, e ainda, por razões de interesse público, devidamente fundamentado, terá o seu registro cancelado, sendo chamados os demais licitantes, respeitada a ordem de classificação.

16.6.1. Quando o preço inicialmente registrado, por motivo superveniente, tornasse superior ao preço praticado no mercado o IDT deverá:

a) convocar os fornecedores visando à negociação para redução dos preços e sua adequação ao praticado no mercado;

b) frustrada a negociação, os fornecedores serão liberados do compromisso assumido;

c) convocar os demais fornecedores visando igual oportunidade de negociação.

16.6.2. Quando o preço de mercado tornar-se superior aos preços registrados e os fornecedores, mediante requerimento devidamente comprovado, não puderem cumprir o compromisso, o IDT poderá:

a) liberar os fornecedores do compromisso assumido, sem aplicação da penalidade, confirmando a veracidade dos motivos e comprovantes apresentados; e

b) convocar os demais fornecedores visando igual oportunidade de negociação.

16.6.3. Não havendo êxito nas negociações, o IDT deverá proceder à revogação da Ata de Registro de Preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

16.7. O licitante deixará de ter o seu preço registrado quando:

a) deixar de cumprir as condições assumidas no instrumento por ele assinado;

b) não aceitar reduzir o preço registrado, quando se tornar superior ao praticado pelo mercado;

c) quando, justificadamente, não for mais do interesse do IDT.

16.8. Após a adjudicação e homologação do resultado, a proponente vencedora será notificada para comparecer em local designado para a formalização da Ata de Registro de Preços, na qual deverá constar, dentre outras condições, o compromisso prestar o serviço na medida das necessidades que lhe forem apresentadas.

16.9. Dentro de prazo de vigência do Registro de Preços, as licitantes que tiverem seus preços registrados ficarão obrigadas ao fornecimento dos serviços, desde que obedecidas às condições deste Edital e da respectiva Ata de Registro de Preços.

16.10. Caso a proponente vencedora não atenda a convocação para assinatura da Ata de Registro de Preços, poderá ser convocada a segunda colocada na ordem de classificação, ou proceder nova licitação.

16.11. O IDT poderá desclassificar a proponente vencedora, caso tenha conhecimento de qualquer fato anterior ou posterior ao julgamento desta licitação que venha desaboná-la técnica, financeira ou administrativamente, não lhe cabendo direito a qualquer reclamação, indenização ou ressarcimento.

16.12. No caso de se constatar a inveracidade de qualquer das informações e/ou documentos fornecidos por qualquer proponente, poderá ele sofrer, a critério do IDT, isolada ou cumulativamente:

16.12.1. Não adjudicação do pedido, sem prejuízo das penalidades previstas, se o Proponente tiver obtido a primeira classificação e a adjudicação ainda não lhe tiver sido efetuada.

16.12.2. Cancelamento do Registro de Preços.

16.12.3. Declaração de inidoneidade com a suspensão do direito de contratação junto ao IDT.

16.13. A Ata de Registro de Preços, durante sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública Municipal, Estadual ou Federal, na condição de órgão Interessado, mediante consulta prévia ao órgão gestor do Registro de Preços e concordância do fornecedor, conforme disciplina os artigos 16 e 18 do Decreto Estadual nº 28.087/2006.

16.14. Os órgãos interessados, quando desejarem fazer uso da Ata de Registro de Preços, deverão manifestar seu interesse junto ao órgão gestor do Registro de Preços, o qual indicará o fornecedor e o preço a ser praticado.

16.15. As contratações decorrentes da utilização da Ata de Registro de Preços de que trata este subitem não poderão exceder, por órgão Interessado, ao somatório dos quantitativos registrados na Ata.

16.16. O fornecedor detentor de preço registrado poderá optar pela aceitação ou não do fornecimento a Órgãos Interessados, desde que este fornecimento não prejudique as obrigações anteriormente assumidas.

17. DA CONTRATAÇÃO

17.1. O Registro de Preços não importa em direito subjetivo à contratação de quem ofertou o preço registrado, sendo facultada a realização de contratações de terceiros sempre que houver preços mais vantajosos ou em função de necessidades não previstas ou por motivo de força maior.

17.2. A Contratada irá responsabilizar-se, em caráter exclusivo, pela prestação dos serviços.

17.3. O IDT convocará a empresa declarada vencedora para assinar o contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo de 05 (cinco) dias, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no art. 81 da Lei 8666/93.

17.4. O contrato terá vigência de **até 12 (doze) meses**, contados a partir data da sua assinatura, podendo ser prorrogado nos termos do § 1º do art. 57, da Lei 8.666/93.

17.5. Não será exigida a prestação de garantia para a contratação resultante desta licitação.

17.6. **A Contratada obriga-se a:**

17.6.1. Fornecer o objeto da licitação, de acordo com as especificações definidas no Termo de Referência. Eventuais alterações deverão ser submetidas à apreciação e aprovação prévia do IDT, devendo estar garantidas, no mínimo, as especificações e certificações exigidas na licitação.

17.6.2. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

17.6.3. Atender a todas as obrigações de natureza fiscal que incidam ou venham a incidir sobre os fornecimentos e distribuições contratados.

17.6.4. Assumir plena e irrestrita responsabilidade por qualquer acidente ou incidente ocorrido, isentando totalmente o IDT de todas e quaisquer reclamações e indenizações que possam surgir em decorrência dos mesmos.

17.6.5. Instruir seu (s) empregado (s) e/ou prepostos, para que, ao entrar (em) nas dependências do IDT, apresente(m) sua identificação ao responsável pela portaria (recepção), para fim de registro.

17.6.6. Notificar o IDT, por escrito, caso ocorra qualquer fato que impossibilite o cumprimento das cláusulas contratuais dentro dos prazos previstos.

17.6.7. Aceitar, nas mesmas condições ora pactuadas, os acréscimos ou supressões que se fizerem necessários no percentual de até 25% (vinte e cinco por cento), do valor inicial atualizado.

17.6.8. Assumir integral responsabilidade pela inexecução parcial ou integral dos serviços prestados, bem como pelos atos omissivos ou comissivos praticados pelos seus empregados, sujeitando às condições e penalidades previstas.

17.6.9. Responsabilizar-se por todo e qualquer espécie de dano causado por seus empregados em face dos serviços, bem como pelo extravio de coisas ocorridas na prestação dos serviços.

17.6.10. Adotar gestões tempestivas, diligentes e imediatas no sentido de corrigir as eventuais falhas ou problemas apurados na execução dos serviços.

17.6.11. Relatar à contratante as ocorrências contratuais.

17.7. **A Contratante deverá assumir as seguintes obrigações:**

17.7.1. Proporcionar todas as facilidades para que a contratada possa realizar os serviços contratados, inclusive planejar as prestações de serviços eventuais.

17.7.2. Assegurar-se da correta cobrança dos serviços, observadas as glosas, antes de cada pagamento, bem como a apresentação dos documentos comprobatórios necessários.

17.7.3. Fiscalizar o cumprimento das obrigações assumidas pela contratada.

17.7.4. Não permitir que outrem execute o objeto contratado, em sua totalidade.

17.7.5. Aplicar penalidades e multas à contratada, mediante o devido processo legal, garantido a ampla defesa e o contraditório.

17.7.6 Efetuar, quando julgar necessário, inspeção com a finalidade de verificar a prestação dos serviços e o atendimento das exigências contratuais.

17.7.7. Comunicar à Contratada toda e qualquer ocorrência relacionada com a execução do serviço.

17.7.8. Exigir, mensalmente, os documentos comprobatórios para o pagamento, conforme especificado no item 12.3. deste Edital.

17.7.9. Emitir as autorizações de execução de serviços, numeradas, assinadas pela autoridade competente.

17.7.10. Efetuar o pagamento à Contratada pelos serviços prestados, nas condições e preços pactuados, à vista da Nota Fiscal/Fatura, devidamente atestada depois de constatado o cumprimento de todas as formalidades e exigências contratuais.

17.7.11. Emitir atestados de capacidade técnica quando solicitados.

17.7.12. Zelar pela pontualidade dos pagamentos decorrentes da execução do contrato, inclusive, aqueles devidos pelos beneficiários.

17.7.13. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da Contratada, que atenderá ou justificará de imediato.

18. DO PAGAMENTO

18.1. O pagamento será efetuado até 10 (dez) dias contados da data da apresentação da Nota Fiscal e Recibo, devidamente atestada pelo gestor da contratação, acompanhada da Autorização de Serviço e da Documentação relativa à regularidade para com a Seguridade Social (INSS), Fundo de Garantia por Tempo de Serviço (FGTS),Trabalhista e Fazendas Federal, Estadual e Municipal, mediante emissão de cheque nominal ou depósito em conta bancária.

18.2. A nota fiscal/fatura que apresente incorreções será devolvida à CONTRATADA para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

18.3. Não será efetuado qualquer pagamento à CONTRATADA**,** em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

18.4. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.

18.5. Caso ocorra, a qualquer tempo, a não aceitação de qualquer parte do fornecimento, o prazo de pagamento será interrompido e reiniciado após a correção pela CONTRATADA.
18.6. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em Cartório. Caso a documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

19. DAS SANÇÕES ADMINISTRATIVAS

19.1. O licitante que praticar quaisquer das condutas previstas no art. 32, do Decreto Estadual nº 28.089/2006, sem prejuízo das sanções legais nas esferas civil e criminal, estará sujeito às seguintes penalidades:

19.1.1. Multa de 10% (dez por cento) sobre o valor da proposta.

19.1.2. Impedimento de licitar e contratar com o Instituto de Desenvolvimento do Trabalho - IDT, sendo, então, descredenciado no cadastro de fornecedores, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste edital e das demais cominações legais.

19.2. O licitante recolherá a multa por meio de pagamento na Tesouraria do IDT podendo ser substituído por outro instrumento legal, em nome do órgão Contratante. Se não o fizer, será cobrada em processo de execução.

19.2.1. As multas porventura aplicadas poderão ser descontadas dos pagamentos devidos pela Contratante ou cobradas diretamente da Contratada, administrativa ou judicialmente, e podendo ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

19.2.2. O atraso injustificado no prazo de fornecimento implicará multa correspondente a 3,33% (três vírgula trinta e três por cento) por dia, calculada sobre o valor total do contrato ou da parcela dos serviços não cumprida, até o limite de **10%** (dez por cento) desse valor.

19.2.3. Na hipótese mencionada no item anterior, o atraso injustificado por período **superior a 05(cinco) dias** caracterizará o descumprimento total da obrigação, punível com a rescisão unilateral do contrato e suas conseqüências, e da aplicação da sanção prevista no item 19.1.2.

19.2.4. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério da Contratante.

19.3. Sempre que não houver prejuízo para a Contratante, as penalidades impostas poderão ser relevadas ou transformadas em outras de menor sanção, a seu critério.

19.4. As aplicações das penalidades serão precedidas de concessões de oportunidades de ampla defesa por parte da Contratada, na forma da lei.

20. DA FRAUDE E DA CORRUPÇÃO

20.1. O Contratado deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos desta clausula, definem-se as seguintes práticas:

a) **"prática corrupta"**: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

b) **"prática fraudulenta":** a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

c) **"prática conluiada"**: esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

d) **"prática coercitiva"**: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato.

e) **"prática obstrutiva":**

(1) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista nesta cláusula;

(2) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

20.2. O contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei nº 8.666/93, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

20.3. Considerando os propósitos dos itens acima, o contratado deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

20.4. O contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei nº 8.666, de 21 de junho de 1993, se compro var o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

21. DO LOCAL E DAS CONDIÇÕES DE FORNECIMENTO DO OBJETO

21.1. O objeto desta licitação deverá ser executado em conformidade com o **ANEXO I** – TERMO DE REFERÊNCIA.

22. DAS DISPOSIÇÕES FINAIS

22.1. As normas disciplinadoras desta licitação serão interpretadas em favor da ampliação da disputa, respeitadas a igualdade de oportunidade entre as licitantes e desde que não comprometam o interesse público, a finalidade e a segurança da contratação.

22.2. Das sessões públicas de processamento do Pregão Eletrônico será lavrada ata circunstanciada.

22.3. O sistema manterá sigilo quanto à identidade das licitantes para o Pregoeiro, até a etapa de negociação com o autor da melhor oferta e para os demais, até a etapa de habilitação.

22.4. O resultado deste Pregão e os demais atos pertinentes a esta licitação, sujeitos à publicação, serão divulgados no Diário Oficial do Estado e nos sítios eletrônicos **www.idt.org.br** e **www.licitacoes-e.com.br**.

22.5. Se for comprovado o não atendimento aos requisitos desta licitação a proponente será desclassificada e/ou inabilitada, conforme o caso.

22.6. Na hipótese de inabilitação e/ou desclassificação de todos os licitantes, o IDT decretará como fracassado o lote ou todos os lotes e poderá relançar os mesmos em novo Edital.

22.7. As condições estabelecidas neste Edital, no que se aplicar, farão parte do contrato correspondente.

22.8. O IDT poderá por interesse próprio, devidamente justificado, cancelar a presente licitação, no seu todo ou em parte, inclusive por vício ou ilegalidade, de ofício ou mediante provocação, bem como adiá-la ou prorrogar o prazo para recebimento das propostas, sem que caiba aos licitantes qualquer direito à reclamação ou indenização.

23. DO FORO

23.1. Para dirimir quaisquer questões decorrentes da licitação, não resolvidas na esfera administrativa, será competente o foro da Comarca da Capital do Estado do Ceará.

24. DOS ANEXOS

24.1. Constituem anexos deste edital, dele fazendo parte:

ANEXO I – TERMO DE REFERÊNCIA

ANEXO II – MODELO DE PROPOSTA COMERCIAL

ANEXO II-A – LISTA DE UNIDADES DO SINE/IDT

ANEXO III – DECLARAÇÃO SIMPLIFICADA

ANEXO IV – DADOS DA EMPRESA E DO REPRESENTANTE LEGAL

ANEXO V - MINUTA DA ATA DE REGISTRO DE PREÇO

ANEXO VI – MINUTA DO CONTRATO

ANEXO VII – TERMO DE CONFIDENCIALIDADE

Fortaleza, 21 de junho de 2016.

Valdenia Maria Andrade Araújo
Presidente

Rosana Barbosa Rodrigues
Pregoeira

Susana Silveira Souza
Apoio

ANEXO I

TERMO DE REFERÊNCIA

01. OBJETO

Registro de Preços para futura e eventual contratação de pessoa jurídica especializada para a Prestação de Serviços Gerenciados de Segurança da Informação, incluindo Monitoração do Ambiente Computacional e Tecnológico do SINE - IDT/CE, conforme detalhamento constante neste Termo de Referência.

02. APRESENTAÇÃO DA SOLUÇÃO

02.01. Trata-se de Prestação de Serviços de Gerenciados em Segurança da Informação, incluindo Monitoração do Ambiente Computacional e Tecnológico do SINE - IDT/CE e decorrentes da utilização de uma Multiplicidade de Soluções e Serviços a serem contratados, estes obrigatoriamente com utilização de SNOC (Security and Network Operation Center). Também e concomitantemente com o provimento de SLA(s) de Atendimento de Chamados, Diagnóstico e Implementação de Gerenciamento Continuado em Segurança de Tecnologia da Informação contemplando: Implementação compreendendo a implantação, fornecimento, configuração, instalação e testes das soluções, Gerência com Monitoramento Remoto em Tempo Integral 24x7x365 (vinte quatro horas por dia, sete dias por semana, todos os dias do ano) e **com obrigatoriedade de Atendimento Presencial de Técnico Certificado e Especializado nas soluções implementadas sempre que necessário junto ao SINE - IDT/CE**. A contratação contempla ainda e também, a Prestação dos Serviços de Emissão de Relatórios das Ferramentas e Serviços ofertados e Suporte Técnico Especializado, durante o período contratual, de todos os Serviços e Soluções aqui previstos e tais como: Firewall com Gerenciamento Unificado de Ameaças (UTM-Unified Threat Management), Solução de Filtro Web com Proxy, Solução de Backup, Correlacionador de Eventos, e Rede Wireless Seguro, **incluindo o conjunto de hardwares e softwares todos eles fornecidos em regime de locação, em quantidades e suficientes para a total e completa prestação desses serviços e todas com a obrigatoriedade de terem funcionamento compatíveis entre si e já, tornando-se público, a exigibilidade de Prova Comprobatória para confirmação das funcionalidades especificadas em todo o âmbito deste instrumento licitatório e também, de acordo com o seguinte escopo:**

a. Solução de Firewall UTM
   i. Serviço de Firewall UTM e aqui denominado Médio e Grande Porte – Tipo I:
   ii. Serviço de Firewall UTM aqui denominado de Pequeno Porte – Tipo II:
b. Serviços de Rede Wireless Segura:
c. Serviço de Backup
d. Serviço de Filtro Web
e. Serviço de Monitoria e Análise Pro Ativa dos Eventos de Segurança

1.1 OBJETIVOS ESTRATÉGICOS

1.1.1 A sociedade, assim como ocorre nas empresas privadas, espera cada vez mais que os órgãos públicos se tornem mais eficientes, seus dirigentes mais comprometidos com os interesses da coletividade requerendo, dessa maneira, um melhor e maior desempenho para o atendimento às crescentes demandas de fornecimento de produtos e serviços de que ela necessita, e que cresce mais rapidamente do que se poderia esperar/imaginar, e encontrando no uso da Tecnologia da Informação, o suporte indispensável para a superação desse desafio e o atendimento imediato às necessidades prementes de serem de imediato satisfeitas.

1.1.2 Os investimentos que se realizam na utilização da TI, possibilitam comprovadamente o aumento da oferta de produtos e serviços além de permitir controles mais efetivos, proteção aos dados dos usuários, facilitação de consultas e interação, melhoria de acesso e utilização dos recursos

computacionais e da Internet, e claro, garantindo a implementação de políticas de gerenciamento adequadas que assegure o controle efetivo da rede, garantindo-lhe o funcionamento estável e seguro, auxiliando diretamente nas tomadas de decisões em todos os níveis da Instituição: administrativo, fiscal, tributário, financeiro, operacional, educacional, social, tecnológico e todos os demais existentes.

1.1.3 Também mediante utilização de tecnologias recentes e adequadas as unidades em funcionamento em diversas localidades do estado têm que assegurar uma conectividade permanente, contínua, operante e segura mesmo quando acessadas a distância e remotamente quando em rede, garantindo a segurança em nível lógico tanto dos equipamentos em utilização na rede de cada unidade, assim como dos dados que por ela trafegam protegendo a incolumidade dos usuários.

1.1.4 Hoje em dia, com a indispensável utilização de ferramentas entre as quais: Correlacionador de Eventos, Firewall, AntiSpam, Inspeção de Conteúdo de Acesso à Internet, Proxy, Antivírus, Sistemas de Prevenção e detecção de Intrusos, Soluções de Endpoint, assim como a utilização da VPN (Virtual Private Networks) dentre outras, que permite a entrada e saída de dados na rede como no caso do SINE - IDT/CE, entre tantos outras ferramentas existentes, objetivam garantir a proteção do ambiente e portanto, tornando-se imperativo a sua ampla utilização, assim como a permanente atualização dessas tecnologias e de outras mais que vêm surgindo ao longo dos últimos anos após o advento da Internet.

1.1.5 Outro ponto a ser considerado é que a aceleração do uso de sistemas na Internet e Mídias Sociais sem controle ou o constante monitoramento podem levar a dispersão dos usuários e a consequente perda de produtividade, da sobrecarga dos recursos da rede lógica das organizações, além de que existem conteúdos na Internet vídeo/áudio que consomem muitos recursos da rede impactando diretamente no tráfego das informações aos usuários em geral e que deve assim ser consideradas.

1.1.6 Já é de pacífico entendimento, tanto nas empresas públicas, privadas, órgão governamentais e a sociedade em geral que atender as crescentes demandas relativas a Tecnologia da Informação obriga por um atendimento responsável, seguro, com alta qualidade e eficiência, com economicidade, confiabilidade, flexibilidade, agilidade e racionalização de fluxo de trabalho que também é uma preocupação constante da direção deste órgão, requer e tornou a Tecnologia da Informação ferramenta estratégica que deve estar alinhada com todas as áreas e em especial, com as áreas de negócios desta Instituição.

1.1.7 Devido ao elevado grau de automação dos processos operacionais e administrativos, as organizações passaram a confiar e a depender cada vez mais de sua infraestrutura tecnológica para viabilizar aplicações de missão crítica e implementar rapidamente novas soluções e serviços que aumentem a agilidade, a capacidade de adaptação, a otimização de custos e a melhoria de serviços prestados, de forma continuada e segura aos seus clientes e usuários em geral.

2. CONTEXTUALIZAÇÃO

2.1. A atual infraestrutura de TI do SINE - IDT/CE se caracteriza por uma grande diversidade de plataformas, sistemas e aplicações, utilizadas para suportar as tarefas relacionadas à gestão estratégica e operacional dos serviços da Instituição e claro, buscando melhoramentos sempre necessários e dar continuidade de forma mais robusta aos nossos serviços de rede inclusive rede cabeada e não cabeada (wifi), além da utilização constante de ferramentas/serviços/soluções essenciais e indispensáveis para a garantia do normal funcionamento da rede, devidamente associada aos requisitos de segurança dos recursos e dos ativos em geral utilizados.

2.2. Para tanto é requerido a contratação de suporte técnico especializado para evitar problemas e, na sua ocorrência, corrigi-los de imediato, também, prover as atualizações disponibilizadas pelos fabricantes, acrescentando a tudo isso o fato de que é inerente à atividade desse órgão a necessidade de termos uma infra-estrutura de rede adequada, incluindo a rede sem fio que será plena e amplamente utilizada porém, de maneira segura.

2.3. No cenário atual, a complexidade e os riscos inerentes aos ambientes tecnológicos, têm gerado crescente aumento nos custos, enquanto que a satisfação dos usuários de tecnologia com a utilização de um suporte adequado e eficiente vem permitindo que o tempo de resposta para a resolução dos

problemas vem decrescendo. Tais constatações estão presentes tanto em organizações públicas quanto nas privadas.

2.4. Diante dessas evidências, tornam-se necessário que as organizações mudem seu enfoque de atendimento aos usuários, de reativo para proativo, alcançando um gerenciamento integrado dos processos envolvidos na entrega e suporte a serviços de Tecnologia da Informação.

2.5. Essa mudança se dá por meio do aumento da aderência das áreas de TI às melhores práticas de mercado, incrementando os processos de gestão dos serviços, aprimorando o controle sobre a infra-estrutura tecnológica e implantando um modelo de governança tecnológica que alcance um gerenciamento proativo e especializado e valorize as soluções sob a perspectiva de atendimento às crescentes necessidades de todas as áreas interessadas e ainda, de forma integrada e segura.

2.6. Esse modelo de governança tecnológica e gestão dos serviços devem ser consolidados através da visão de futuro da organização como base de orientação para a definição dos objetivos e metas estratégicas que devem ser suportadas pelos Serviços e pela Infra-estrutura de Tecnologia da Informação, a única responsável por manter o negócio em pleno e seguro funcionamento para satisfazer as muitas e crescentes demandas de todas as áreas da Instituição aqui enfocando seu público interno e externo.

2.7. Nas organizações públicas no âmbito Federal, Estadual e Municipal, a implantação de modelos de Governança e Políticas de Segurança da Informação, vem sendo requeridas em auditorias realizadas pelos órgãos de controle sobre as áreas de TI dessas organizações, não mais sendo permitindo alegativas/ justificativas pela não utilização, assim como a não contratação de serviços e soluções de TI.

2.8. A definição de um novo patamar qualitativo para a Gestão dos Serviços de TIC constitui hoje o maior desafio contemporâneo das áreas de Tecnologia da Informação e Comunicação quer sejam nas organizações públicas e/ou privadas no Brasil e no mundo.

3. JUSTIFICATIVAS PARA CONTRATAÇÃO DOS SERVIÇOS

3.1. A contratação das tecnologias aqui precificadas justifica-se então, pelas seguintes necessidades, entre outras mesmo que aqui não mencionadas e objetivam a obtenção das melhores práticas em relação aos serviços e soluções que deverão ser implementados pela Licitante Vencedora e buscam a/o:

3.1.1. Liberação seletiva/controlada de acesso às mídias sociais e mídias de comunicação através da constante utilização da Internet visando o uso dos recursos de rede de forma otimizada e com segurança.

3.1.2. Controle do acesso permitindo a seletividade do processo no que diz respeito aos usuários e conteúdos aceitáveis.

3.1.3. Cumprimento às exigências previstas neste edital para utilização de Centros de Operações de Segurança de Rede - SNOC (Security Network Operation Center) que visa a obtenção de um atendimento especializado e eficiente, gerenciado e monitorado por profissionais capacitados e certificados com as mais conceituadas certificações, capacitados para manter os sistemas em pleno e normal funcionamento, além de segurança da organização e funcionando dentro dos objetivos e das especificações desejadas e necessárias.

3.1.3.1. Permite e visa a obtenção de uma maior segurança de dados assim como a integridade das informações mediante o Monitoramento Remoto dos Serviços e Soluções implantados. Através dele disponibiliza-se Soluções Inteligentes para Segurança do Sistema de Informação no período 24 horas por dia, 7 dias por semana, todos os dias do ano, alertando o surgimento de problemas e permitindo sua imediata resolução, estando seus requisitos pormenorizados no contexto deste edital.

3.1.3.2. Toda a infra-estrutura de hardwares e softwares do SNOC da Contratada para a prestação dos serviços descritos deverão se encontrar em funcionamento em um Datacenter com alta disponibilidade de serviços e segurança de dados na data de publicação deste edital, para permitir seu normal, integral e seguro funcionamento. Os atendimentos às demandas do SINE – IDT/CE deverão ser gerenciados e atendidos através de processo que priorize os chamados e que, por sua

vez, estarão caracterizados e definidos pelos Níveis de Serviços, também pormenorizados no contexto deste edital.

3.1.3.3. Por meio do relacionamento com a equipe atuante no SNOC, benefícios outros ocorrerão com análises e avaliações, viabilizando a busca por necessidades que resultarão em novos projetos e aperfeiçoamento das práticas de segurança implantadas e a serem implementadas.

3.1.3.4. O serviço de Operações de Segurança de Redes (SNOC) devem ser fornecidos pela CONTRATADA voltado e contemplando, sem exceção também a monitoração, análise e prevenção de ataques cibernéticos.

3.1.3.5. Os serviços de Operações de Segurança de Redes devem possuir profissionais treinados e certificados nas principais práticas e procedimentos em segurança da informação existentes no mercado, possuindo ainda acesso à base externa de informações sobre últimos ataques e vulnerabilidades.

3.1.3.6. O serviço de monitoramento de eventos de segurança, análise e prevenção de ataques cibernéticos inclui, mas não se restringe, a alertas de:

a) Ataques de força bruta com e sem sucesso;

b) Infecção de equipamentos por vírus;

c) Comprometimento / invasão de ativos da rede;

d) Realização de ações suspeitas por parte de usuários privilegiados;

e) Alertas de operação de serviços, como interrupções e falhas;

f) Ataques de negação de serviço (DoS e DDoS);

g) Falhas de autenticação;

h) Autenticações concorrentes de múltiplas regiões ou cidades com as mesmas credenciais (roubo de identidade);

i) Ataques comuns em aplicações WEB, como XSS e SQL injection;

j) Atividades de botnets;

k) Identificação em tempo real e de maneira automatizada a origem dos eventos de segurança, identificando cidade, estados e países e não somente os endereços IP de origem;

3.1.4. O Gerenciamento dos Serviços de TI é um método dinâmico para relacionar os componentes e serviços de TI aos objetivos e metas da Instituição. Este método trará como benefício permitir identificar os serviços críticos de TI sobre os quais as atividades o SINE - IDT/CE dependem; serviços que, no geral, são realizados por muitas aplicações de alta criticidade, bancos de dados que guarnecem a incolumidade dos dados, servidores que processam grandes volumes de informações, switches, e diversos muitos outros elementos de rede. Identificar também tais serviços críticos irá permitir dentre diversas atividades a definição de uma política clara e objetiva para Segurança da Informação e Gestão dos Ativos de Tecnologia da Informação do SINE - IDT/CE.

3.1.4.1. Desta forma, será possível planejar e entender como os serviços disponibilizados pela TI impactam os serviços corporativos do SINE - IDT/CE, mitigar seus riscos e necessidades de planos de gestão e contingência. Além disso, serão obtidos outros resultados, como por exemplo: a melhoria no desempenho dos serviços e a redução do custo e complexidade da infra-estrutura de TI, bem como o pleno atendimento às regulamentações do setor que atualmente exigem cada mais a implementação de recursos de TI associados a uma gestão eficaz, responsável e a mais segura possível.

3.1.4.2. Neste contexto os incidentes podem ser rapidamente relacionados à causa raiz porque as entidades de negócios descritas pelos usuários já estarão relacionadas à infra-estrutura de TI. As modificações nos serviços e na infra-estrutura poderão ser planejadas e controladas para otimizar a disponibilidade e a segurança dos serviços. Finalmente, a aderência às regulamentações estará/será assegurada porque os processos e os recursos necessários para executá-los serão identificados e documentados, este é mais um benefício substancial a ser atingido.

3.1.4.3. A utilização de uma rede sem fio (wireless) segura e flexível permitirá aos usuários mobilidade, esta que atualmente é imprescindível e hoje se constituindo em um requisito indispensável ao SINE - IDT/CE.

3.1.5. A implantação de controles, de forma a proteger e manter disponível a comunicação de dados, onde se faz uso cada vez mais, a cada dia, dos recursos de Internet, necessita e obriga a se estabelecer/utilizar recursos avançados de Filtros de Conteúdo, Prevenção a Conteúdos Maliciosos ou de uso improdutivo tais como P2P, Chat, Proxy Anônimos, Radio, Streaming de Vídeos, Games entre outros, e ainda, um sistema de gerenciamento de ferramentas de comunicação como do tipo Messenger, armazenamento, configurável, para garantir que a Internet seja utilizada em conformidade com os objetivos e as políticas estabelecidas pelo órgão, com destaque para a segurança dos dados e de infra-estrutura de TI.

3.1.6. A existência de uma empresa que possa vir a ser contratada e que forneça garantia e suporte especializados suficientes e capazes para suportar a complexidade de nossa estrutura e atividade interdependentes da TI visa manter os Serviços e Soluções a serem contratadas em correto, completo, normal e seguro funcionamento e sempre de maneira disponível, atualizada e responsável.

3.1.7. Importante também enfatizarmos que não há/haverá duplicidade de investimentos em relação às anteriores soluções de TI, uma vez que se trata de soluções diferentes, indispensáveis, e estas, objeto deste pregão, se destinam ao atendimento das necessidades complementares, aqui tratadas.

3.1.8. O formato de se licitar em lote único se faz necessário e obrigatório e se dá pela necessidade de compatibilidade e integração entre todos os itens requeridos, sendo assim indispensável que todas as soluções definidas por esse documento sejam entregues por um único fornecedor para a prestação dos múltiplos serviços requeridos, evitando-se futuros conflitos que certamente ocorrem quando diversos fornecedores atendendo a demandas distintas de tecnologias atuam no mesmo ambiente, que acaba permitindo a ocorrência de incidentes visto que interpretações, conhecimentos, procedimentos e processos não são convergentes ou alinhados e sim particularizados. Não se pode também desconhecer que quando se utilizam uma gama de serviços e soluções de TI tem que se ter em busca a melhor prestação de serviços gerenciados e a indispensável interoperabilidade dos mesmos, como no presente caso.

4. DESCRIÇÃO DOS SERVIÇOS

4.1. A Licitante Vencedora deverá cumprir com todos os requisitos especificados no todo deste edital, e sem nenhuma exceção, sob pena de desclassificação imediata e atendendo a tudo quanto também estará abaixo elencado, no que se refere aos serviços a serem prestados e ora objeto deste edital:

4.2. Implantação das Soluções

4.2.2. A Contratada deverá realizar a prestação dos serviços e implantação das soluções, mediante solicitação e com configuração, instalação, testes e fornecimentos dos hardwares e softwares relacionados, em regime de locação, para todas as soluções e serviços contratados através de utilização obrigatória de SNOC e profissionais capacitados e certificados pelos fabricantes.

4.2.3.Todas as atividades envolvidas e decorrentes da prestação dos serviços e implantação das soluções serão devidamente acompanhadas e coordenadas por analistas e técnicos do SINE - IDT/CE.

4.2.4. A implantação das soluções, quando realizadas no ambiente de produção, poderá exigir a necessidade de que as atividades sejam realizadas após o expediente (horários noturnos e/ou em finais de semana e feriados) a fim de não comprometer o normal funcionamento das atividades do SINE - IDT/CE.

4.2.5. A Contratada será responsável por efetuar as atividades de integração de todas as soluções aqui previstas, especialmente quanto aquelas de monitoração remota, de service desk, correlação de eventos e todas as demais no ambiente operacional do SINE - IDT/CE, sem prejuízo aos serviços deste e nas localidades e onde o SINE - IDT/CE solicitar.

4.3. Prestação dos Serviços Contínuos

4.3.1. Os serviços poderão ser prestados remotamente, não estando excluída a prestação de serviços in loco (significando dizer, na língua pátria: no local) de técnicos capacitados e certificados da Contratada e diante de solicitações que venham a ocorrer.

4.3.1.1 O suporte técnico e atendimento remoto serão executados obrigatoriamente a partir de 2 (dois) Centros de Operação de Segurança e Redes (SNOC) redundantes da Contratada, sendo o primeiro localizado em Fortaleza/Ce e o segundo necessariamente em outro estado da Federação, para permitir plena operacionalidade em vista de eventual ocorrência de parada de um deles.

4.3.1.2 Os referidos Centros de Operação serão objeto de comprovação documental conforme item 5 deste Termo, e se necessário também, através de diligências que serão efetuadas por técnicos do SINE-IDT/CE, sendo igualmente exigida a comprovação da existência de todos os requisitos especificados neste documento, inclusive, a obrigatoriedade de já estar em pleno funcionamento na data da publicação do edital.

4.3.2. Os serviços de monitoração remota das soluções e serviços aqui contemplados deverão ser realizados pela Contratada, na modalidade 24x7x365 (vinte e quatro horas por dia, sete dias na semana, todos os dias do ano). Há previsibilidade de interação presencial no caso de necessidades que possam vir a ocorrer e sem limite para tanto.

4.3.3. Para a manutenção dos hardwares e softwares ofertados, bem como para a prestação do suporte técnico aos serviços de monitoração remota, a Contratada deverá já possuir infra-estrutura de suporte técnico, disponível em período integral, ou seja, 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), nos seguintes modelos:

4.3.3.1. Suporte técnico remoto: suporte prestado por meio de Central de Atendimento 0800 ou equivalente à ligação local para:

4.3.3.2. Esclarecimento de dúvidas relacionadas à prestação dos serviços, políticas e regras implementadas, funcionalidade das soluções e incidentes de segurança, sendo este atendimento imediato.

4.3.3.3. Atendimento às solicitações de alterações (inclusão e exclusão) de políticas e regras. Atendimento às solicitações de log e relatórios.

4.3.3.3.1. Suporte técnico local: atendimento in loco, prestados por técnicos capacitados e certificados em quantidade suficiente para prestar todos os serviços conforme estabelecido no contexto geral deste edital, para a solução de eventuais problemas relacionados aos serviços, equipamentos, soluções e softwares ofertados.

4.3.4. As versões dos softwares ofertados pela Contratada sempre deverão estar com a versão mais atual disponível no mercado. A versão anterior:

4.3.4.1. Não poderá permanecer instalada mais do que 3 (três) meses, após o lançamento da última versão homologada; ou

4.3.4.2. Poderá permanecer instalada por tempo maior, desde que acordado com o SINE-IDT/CE.

4.3.5. A Contratada deverá disponibilizar sem ônus adicional, para utilização nas instalações do SINE - IDT/CE, de até 4 (quatro) telas de LCD de 40" para permitir a visualização e o acesso de leitura a console de gerenciamento e monitoramento de todas as soluções ofertadas cujas implementações também serão de responsabilidade única da Contratada.

4.3.6. Serão apresentados pela Contratada, no mínimo, relatórios analíticos mensais contendo o diagnóstico dos ambientes monitorados, obtido através do cruzamento das informações coletadas pelos softwares destinados a esse fim e de responsabilidade exclusiva da Contratada. Tais relatórios deverão estar disponíveis para o SINE - IDT/CE a qualquer momento, se solicitado, devendo ser disponibilizados em até 24 (vinte e quatro) horas após a solicitação.

4.3.7. Os recursos humanos envolvidos nas atividades de monitoração remota da segurança deverão ser suficientes e dedicados às atividades de monitoração e de pleno conhecimento e reconhecimento por parte do SINE-IDT/CE, ou seja, estando sempre disponíveis para executar as atividades exigidas no contexto geral deste edital, mormente porque ocorrerá certamente atendimentos presenciais.

4.3.8. Os recursos humanos envolvidos na prestação de serviço de monitoração e suporte técnico das soluções e serviços contratados deverão conhecer e estar capacitados e certificados em todas as soluções contempladas neste edital. Entende-se por capacitação: **certificados e/ou atestados profissionais emitidos pelos fabricantes e/ou distribuidores oficiais dos fabricantes ou instituições independentes que deverão ser apresentados na proposta.**

4.3.9. A Contratada deverá interagir com os analistas e técnicos do SINE-IDT/CE para dirimir/explicitar/equacionar dúvidas/questionamentos relacionadas aos serviços prestados, mediante atendimento telefônico por central 0800 ou equivalente à ligação local, assim como na forma presencial quando solicitada.

4.3.10. A Contratada deverá disponibilizar também um sistema de abertura de chamados via WEB com aderência as melhores práticas ITIL conforme descrito no item 4.3.10.1. e seguintes. A Licitante deverá informar todo processo de abertura de chamados. Esta comprovação deverá ser realizada já na fase de apresentação dos documentos de habilitação e não ocorrência da referida comprovação será motivo suficiente para a desclassificação da mesma, ato contínuo.

4.3.10.1. A ferramenta a ser utilizada para gestão de todo o processo de atendimento de chamados (Service Desk) deverá no mínimo, conter/apresentar as funcionalidades mínimas conforme abaixo descritas:

4.3.10.1.1. A plataforma deve comprovar aderência, no mínimo ao **ITIL 2011** através da apresentação da certificação PinkVerify para os processos de Gerenciamento de Incidentes, Requisições e Catálogo de Serviços.

4.3.10.1.2. Deve possuir estrutura de desenvolvimento, manutenção e suporte da ferramenta no Brasil.

4.3.10.1.3. O software deve possuir documentação online para permitir acesso a consultas, também sendo capaz de orientar seus usuários e contendo às informações de conteúdo no idioma Português/Brasil.

4.3.10.1.4. Suportar a abertura de chamados mediante a utilização de aplicação nativa para dispositivos móveis baseados em Android e IOS.

4.3.10.1.5. Possibilitar utilização de relatórios e estatísticas através da definição de filtros de pesquisa diretamente na interface do software e sem necessidade de software adicional.

4.3.10.1.6. Possibilitar a impressão de relatórios, estatísticas e resultados de pesquisas.

4.3.10.1.7. Garantir a definição de controles de níveis de acesso aos dados quando da elaboração/confecção dos relatórios.

4.3.10.1.8. Permitir a inclusão de logotipo da Contratante em telas e relatórios, com base em parametrização.

4.3.10.1.9. Permitir a exibição de indicadores em formato de gráficos com as respectivas definições de faixas de valores de forma configurável.

4.3.10.1.10. Possuir recursos para constituição de uma base de conhecimentos técnicos, operacionais, normativos e administrativos.

4.3.10.1.11. Possibilitar o fornecimento para cada registro um número único, registrando também a data e hora de abertura e data e hora da última atualização dos registros de incidentes e requisições de serviços.

4.3.10.1.12. Possibilitar ao atendente que estiver fazendo uso da interface do Software, classificar o impacto e a urgência de sua solicitação de acordo com uma pré-configuração.

4.3.10.1.13. Permitir que a classificação/ categorização possa ser alterada, a qualquer tempo e por quem for autorizado, mantendo, porém, o registro das alterações para consultas futuras.

4.3.10.1.14. Possibilitar a definição automática de prioridade do chamado de acordo com o nível de interrupção de serviço informado.

4.3.10.1.15. Possibilitar a definição de tempos de atendimento (SLA's) contendo os parâmetros de prazos de respostas e resolução dos incidentes/requisições, conforme a severidade associada e precificada neste edital.

4.3.10.2. Os chamados abertos só poderão ser fechados após autorização de funcionário designado pelo SINE-IDT/CE e deverão aguardar um prazo mínimo de 2 (dois) dias para a aprovação por parte da Contratante.

4.3.10.3. O SINE-IDT/CE informará as pessoas autorizadas a abrir e fechar chamados junto à Contratada.

4.3.10.4. A Contratada será responsável, sem ônus adicional ao SINE-IDT/CE por ministrar **treinamento para até 7 (sete) pessoas pertencentes ao quadro funcional do IDT** para as Soluções de Firewall, através de Instrutor Oficial do Fabricante, ficando facultado, a critério exclusivo do SINE-IDT/CE a solicitação para aplicação do exame oficial para certificação em Centro de Certificação Oficial, também sem qualquer ônus adicional.

4.3.11. Manutenção das Regras e Políticas e versões dos Softwares

4.3.11.1. Toda e qualquer alteração na configuração das soluções (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de "patches", entre outras correlatas) deverá ocorrer mediante autorização do SINE-IDT/CE.

4.3.11.2. O SINE-IDT/CE, no momento da implantação das soluções, indicará as pessoas que poderão autorizar as referidas alterações.

4.3.12. As alterações das configurações deverão ocorrer em horários determinados pelo SINE-IDT/CE.

4.3.13. O tempo de atendimento às solicitações de alterações das políticas e regras feitas pelo SINE-IDT/CE não deverá ultrapassar o SLA (Acordo de Nível de Serviço) especificado neste documento, a contar da efetivação das solicitações.

4.3.14. A Contratada deverá efetuar, em laboratório próprio, os testes necessários antes de implementação de qualquer alteração no ambiente de monitoração (políticas, regras, versões e correlatos), evitando impactos negativos nos serviços do SINE-IDT/CE salvo se, pela urgência este último dispensar os testes preliminares.

4.3.14.1. Caso sejam solicitadas alterações substanciais na configuração e forma de aplicação das tecnologias especificadas no edital, o SLA para tais solicitações poderá ser prorrogado a fim de permitir a devida execução de testes e validação das configurações visando garantir a correta implementação para o bom e regular funcionamento das soluções.

4.3.14.2. O SINE-IDT/CE poderá solicitar a qualquer tempo e por escrito, o acesso às senhas de configuração dos equipamentos disponibilizados pela Contratada em regime de locação. O SINE-IDT/CE designará duas pessoas para terem acesso às senhas, que devem ser fornecidas de forma segura. O SINE-IDT/CE 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 diante da possibilidade de ocorrência de acessos.

4.3.15. Controle dos Serviços Realizados pela CONTRATADA

4.3.15.1. Para o controle e administração dos serviços realizados pela Contratada, o SINE-IDT/CE poderá nomear até 3 (três) representantes autorizados a interagir com aquela. Tais representantes serão responsáveis por:

4.3.15.1.1. Manter as informações técnicas (configuração do ambiente) atualizadas, bem como dar suporte na implantação e manutenção das soluções a serem utilizadas.

4.3.15.1.2. Definir as estratégias, políticas e regras a serem implantadas, além de analisar os relatórios gerados pelos softwares que compõem as soluções ofertadas.

4.3.15.1.3. Tomar todas as providências necessárias em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência, por exemplo).

4.3.16. Para cada solução implantada a Contratada emitirá relatórios definidos pelo SINE-IDT/CE, mas em conformidade com as informações nele disponibilizadas pelo fabricante, este o responsável pela fabricação do software a ser utilizado.

4.3.16.1. A Contratada poderá, caso seja solicitado, realizar reuniões mensais, nas dependências do SINE-IDT/CE para dirimir quaisquer dúvidas sobre os serviços contratados, análise e

entendimento dos relatórios gerenciais e administrativos e revisão das configurações e procedimentos implementados. Para tanto, agendará as datas das reuniões com antecedência mínima de 5 (cinco) dias corridos da data desejada mais próxima.

4.3.16.2. O SINE-IDT/CE poderá, a qualquer tempo realizar auditoria nas instalações dos Centros de Operações de Segurança e Rede (SNOC), com o objetivo de verificar as instalações físicas, a segurança física e lógica do ambiente, e demais itens exigidos neste documento, desde que previamente acordada com a Contratada.

4.3.17. Ocorrência de Incidentes

4.3.17.1. No caso de detecção de algum incidente de segurança, a Contratada pode acionar o SINE-IDT/CE imediatamente, para que sejam tomadas as medidas corretivas e legais necessárias, de acordo com o procedimento de resposta a incidentes aqui especificados.

4.3.18. Serão considerados incidentes de segurança, por exemplo: 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 SINE-IDT/CE.

4.3.18.1. A Contratada deverá comunicar imediatamente o SINE-IDT/CE, para que possa ser tomada ações preventivas, nos casos de tentativas de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha colocar em risco a segurança do ambiente do SINE-IDT/CE, mesmo que a ocorrência não tenha logrado êxito/ sem sucesso, mas que seja detectada a insistência por parte da pessoa mal intencionada.

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

4.3.18.1. Dependendo do grau do incidente, a Contratada deverá deslocar recursos técnicos capazes de dar suporte *in loco* objetivando, de imediato, resolução ao problema, para compor o tempo de resposta do SINE-IDT/CE, visando também dirimir quaisquer dúvidas e dar suporte nas providências a serem customizadas.

4.3.19. Soluções de Hardware e Software da CONTRATADA

4.3.19.1. Os Softwares e Hardwares necessários para implantação do serviço de monitoração, gerência e administração remota das soluções de segurança ofertadas fazem parte dos serviços a serem prestados pela Contratada durante o prazo de vigência do Contrato e sendo de sua exclusiva responsabilidade quanto a aquisição, manutenção, atualização vez que o modelo de contratação prevê a locação deles.

4.3.19.2. A manutenção das Licenças dos Hardwares e Softwares necessários, junto aos fabricantes, será de responsabilidade da Contratada, devendo esta apresentar cópia autenticada de aquisição das mesmas, anualmente ao SINE-IDT/CE.

4.3.19.3. Os Hardwares e Softwares ofertados deverão ser totalmente compatíveis com o ambiente operacional do SINE-IDT/CE, não sendo assim aceito, em nenhuma circunstância em caso de incompatibilidade de qualquer ordem a fim de se manter a interoperabilidade de todos os recursos em utilização.

4.3.19.4. A Contratada é/ será sempre a única responsável por atividades que tenha como objetivo a manutenção preventiva e corretiva dos Hardwares por ela ofertados.

4.3.19.5. Tanto os Hardwares quanto os Softwares utilizados/ a serem utilizados devem ser fornecidos em regime de locação como já amplamente mencionado e entendido no contexto geral deste edital.

4.3.20. Encerramento dos Serviços de Monitoração Remota da Segurança

4.3.20.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a Contratada deverá retirar os componentes da solução, comunicando a retirada ao SINE-IDT/CE, por escrito, com 30 (trinta) dias de antecedência.

4.3.20.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para o SINE-IDT/CE, em mídia magnética ou via rede, e em seguida eliminadas da base de dados da Contratada.

5. DAS CONDIÇÕES MÍNIMAS EXIGIDAS PARA A PRESTAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS

5.1. **Os Centros de Operação de Segurança e Rede (SNOC)** já devem estar em pleno funcionamento na data da abertura deste edital e possuir alta disponibilidade além de atender a TODOS os requisitos aqui especificados no contexto geral deste Edital, sob pena de desclassificação sumária da LICITANTE que não atender e especialmente quanto aos demais seguintes requisitos, abaixo enumerados:

5.1.1. Os ativos de TI empregados/ que venham a ser utilizados no monitoramento (como por exemplo: servidores, switches, sistemas de comunicação e demais infra-estrutura de rede e softwares) deverão estar hospedados obrigatoriamente em ambiente seguro – Datacenter -, que atenda, no mínimo e sem exceção, as seguintes especificações mínimas obrigatórias:

5.1.1.1. Possuir sistemas redundantes para armazenamento de dados.

5.1.1.2. Localização: As unidades devem estar localizadas fora de zonas de riscos, ou seja, estar em local que não possua histórico de alagamentos nos últimos 3 (três) anos e deve estar fora da zona de pousos e decolagens de aeronaves.

5.1.1.3. Segurança Física: Disponibilidade de equipe dedicada, treinada, capacitada e certificada e que será responsável pela segurança de acesso a unidade e aos equipamentos lá existentes. Por sua vez o Controle de Acessos deverá ser realizado na entrada e saída de pessoas que acessem e façam uso da unidade através de Sistema Biométrico. Deverá possuir Câmeras de Circuito Interno de Televisão (CFTV), devidamente monitoradas e gerenciadas, cujas imagens possam ser posteriormente consultadas e viabilizem o rastreamento de pessoas que adentrarem a unidade.

5.1.1.4. Energia Elétrica: As Instalações Elétricas da unidade deverão ter total independência no fornecimento de energia na eventualidade de falha na subestação, através de solução de grupo gerador, com acionamento automático na eventualidade de interrupção no fornecimento de energia elétrica e com capacidade mínima de funcionamento por 24 (vinte e quatro) horas.

5.1.1.5. O Sistema de Baterias deverá ser redundante para garantir a transição entre o fornecimento normal de energia e a entrada em operação do grupo gerador.

5.1.1.6. Climatização: Conter um Sistema de Climatização com controles de temperatura e monitoração da umidade relativa do ar, de forma a manter a temperatura constante de 20ºC +/- 2ºC e umidade relativa do ar constante de 50% +/- 10% na área onde estarão funcionando/abrigados os ativos, no interior da unidade.

5.1.1.7. Sistema de Proteção de Incêndio: A unidade devera possuir Sistema e Solução de Combate a Incêndio com sensores de fumaça, extintores de incêndio e sistema gasoso, que permita uma ação rápida e eficiente no combate a possíveis focos de incêndio. A extinção de incêndio deverá ser feita com métodos que não prejudiquem ou afetem/inutilize o funcionamento dos equipamentos, como por exemplo com utilização de sistemas gasosos do tipo FM200.

5.1.1.8. O Data Center deverá possuir no mínimo 2 (dois) links de Internet de operadoras diferentes e com capacidade mínima de 50 Mbps. Deverá ser provido um Link de Comunicação direta com o SINE-IDT/CE, do tipo ponto a ponto ou MPLS, com velocidade mínima de 10 Mbps.

5.2. Licitante deverá possuir em seus Centros de Monitoramento Remoto uma **plataforma que permita aferir a performance e disponibilidade dos ativos** (processamento, memória, número de conexões, dentre outras), servidores e aplicações e que atenda aos requisitos mínimos descritos abaixo:

5.2.1. A Plataforma de Monitoramento deverá permitir a monitoração de firewalls, switches, roteadores servidores e demais equipamentos de rede, a partir de um servidor central, possibilitando a geração de notificações específicas para cada equipe, através de acesso web à aplicação de gerenciamento com as seguintes características:

a) A interface de gerenciamento deverá ser em modo WEB acessada através de browser;

b) Permitir que as informações gerenciadas, coletadas em diversos pontos de captura, sejam consolidadas em uma única visão em um console gráfico central.

c) Possuir a capacidade de reiniciar serviços de monitoração automaticamente após a ocorrência de "queda" e alertar em sequência o retorno da máquina que está sendo gerenciada.

d) Deverá ter capacidade de monitoração de, no mínimo, os seguintes elementos, objetos ou serviços que abranjam a Estrutura de TI: disco (Windows ou Linux), memória ram, Tráfego de interfaces de rede, CPU, número de conexões/processamento/memória do firewall e processos que estão sendo executados nos servidores.

5.2.2. Monitoramento de sistemas operacionais Linux:

a) Utilização de CPU;
b) Memória física e virtual utilizada;
c) Status de Serviços;
d) Espaço livre/utilizado nos discos;
e) Uptime;

5.2.3. Monitoramento de sistemas operacionais Microsoft:

a) CPU;
b) Memória física e virtual utilizada;
c) Status de serviços;
d) Espaço em disco;
e) Uptime;

5.2.4. Monitoramento de Banco de dados SQL Server;

a) User Connections
b) Logins
c) Logouts
d) Full Scans
e) Page Splits
f) Table Lock Escalations
g) Buffer Cache Hit Ratio
h) Database Pages
i) Stolen Pages
j) Page Life Expectancy
k) Connection Memory (KB)
l) Optimizer Memory (KB)
m) Total Server Memory (KB)
n) Target Server Memory (KB)
o) SQL Cache Memory (KB)
p) Lock Requests
q) Deadlocks
r) Average Wait Time
s) Batch Requests
t) SQL Compilations
u) SQL Re-Compilations

5.2.5. Monitoração de roteadores, switches e appliances de rede via SNMP:

a) Detecção de interfaces UP e DOWN

b) Percentual de utilização de interfaces, percentual de erros in/out, percentual de pacotes descartados in/out;

c) Qualquer item disponível nas MIBs Standard;

d) Qualquer item disponível nas MIBs ambientais, como percentual de load do processador, temperatura do dispositivo, velocidade do cooler, etc.

5.2.6. Gatilhos e alertas:

a) A Plataforma deve permitir a construção para a detecção de eventos (gatilhos) de acordo com a necessidade de gerenciamento dos sistemas, gerando os alertas necessários. Como exemplo, ela deve permitir a criação de gatilhos quando limites forem excedidos, quando transações travarem ou quando ocorrem excessivos atrasos no acesso ao banco de dados. Os alertas devem ser configuráveis para criação de SLAs. Os alertas devem ser visualizados também pela interface gráfica.

b) O envio de e-mail e SMS devem ser configurados por tipo de alerta em cada recurso monitorado, permitindo, por exemplo, que em diferentes discos de um mesmo servidor tenham gatilhos e forma de envio diferente.

c) Prover o envio de alarmes para a console de gerenciamento de aplicações e e-mails e SMS para os administradores quando os recursos monitorados atingirem os seus respectivos gatilhos.

d) Para o mesmo item podem ser gerados vários gatilhos com criticidade diferentes, permitindo assim, um melhor controle do tipo de problema.

e) Possuir processo de coleta que, preferencialmente, não instale agentes nos objetos monitorados, a não ser em caso de real necessidade.

5.2.7. Análise, relatórios e comparação:

a) Armazenar informações para posterior análise, permitindo fazer comparações para acertos no ambiente. A solução deverá possuir uma interface interna para geração de relatórios. A solução deve possuir interface web para geração e visualização de relatórios. A interface web deve possibilitar o envio de relatórios por e-mail manualmente ou mesmo pré-agendar a geração e o envio em uma data ou horários especificados. A solução deve possibilitar a exportação dos relatórios nos seguintes formatos:

- PDF
- HTML
- CSV

b) Permitir a filtragem de informações por horário, aplicação ou servidor, sem a necessidade de codificação de scripts para este fim.

c) Todos os relatórios devem ter a flexibilidade de exibir informações em tempo real e também dados históricos, coletados em períodos anteriores.

d) A solução deve permitir a publicação automática de relatórios no formato HTML em um servidor Web, permitindo uma análise sobre a situação dos servidores monitorados, com as seguintes características:

- Apresentação dos nomes dos servidores no relatório;
- Apresentação das informações gerenciadas por servidor;
- Exibição por grupo de servidores previamente estabelecidos;
- Opções de periodicidade especificada pelo usuário: diária, semanal, mensal, trimestral, anual ou intervalo de data;
- Apresentação em modo gráfico.

e) A solução deverá permitir a criação de gráficos unitários ou em conjunto de qualquer item de monitoramento, permitindo assim, uma análise cruzada entre os vários dados monitorados, por exemplo: Colocar no mesmo gráfico o consumo de CPU de um servidor Windows e o consumo de disco de um servidor Linux. Tudo isso de maneira intuitiva e sem a necessidade de customizações.

f) Dependência entre objetos monitorados: Permitir que sejam cadastradas dependências entre os objetos monitorados, inclusive no nível de subitem de monitoramento, permitindo analisar o impacto de uma parada perante os demais objetos monitorados. Quando do cadastramento de uma manutenção preventiva de qualquer um dos objetos monitorados, todos os grupos responsáveis pelos objetos dependentes devem ser informados.

g) Monitoração: Permitir o monitoramento de, no mínimo, os seguintes dispositivos, sistemas e recursos: Sistema Operacional Microsoft Windows 2003/2008 x86/x64, Sistema Operacional Linux, Banco de Dados Microsoft SQL Server 2005 ou superior, Banco de Dados PostgreSQL, Microsoft Exchange Server 2007, Microsoft IIS 6/7, Storage Dell, Roteadores Cisco, Switches HPE dentre outros appliances de rede via protocolo SNMP, No-Breaks gerenciáveis via SNMP, Firewall, Conexão de Portas TCP, Ping e TraceRoute.

5.3. Equipe de Profissionais

5.3.1. A Contratada deve possuir e estar pronta a fornecer pessoal suficiente, necessário e tecnicamente habilitado, capacitado e certificado em todas as soluções a serem utilizadas visando à boa, normal e integral implementação, execução, manutenção e completa e seguro operacionalidade dos serviços contratados.

5.3.2. A Contratada deve fornecer todos os materiais e serviços próprios e adequados à execução dos trabalhos necessários.

5.3.3. A Contratada deve retirar da prestação dos serviços qualquer empregado que, a critério do SINE-IDT/CE, seja julgado inconveniente/ inoportuno/ indesejado ao bom andamento dos trabalhos e dos serviços contratados.

5.3.4. 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 a pena de serem tais dificuldades consideradas inexistentes.

5.3.5. Além das qualificações exigidas para cada serviço prestado, a Contratada deverá ter, no mínimo, profissionais com os certificados especificados na Tabela 1 mais abaixo e de forma a garantir a prestação adequada dos serviços de Segurança da Informação previstos:

Perfil do Profissional	Certificação	Quantidade mínima de profissionais certificados
Consultor Sênior de Segurança	Certified Information Systems Security Professional (CISSP)	01
Consultor de Segurança	CompTIA Security+	02
Consultor em Tecnologia da Informação – Infraestrutura de Rede	CompTIA Network+ ou CCNA – Cisco Certified Network Associate	02
Consultor em Tecnologia da Informação – ITIL	ITIL Foundation Certified	03
Consultor em Tecnologia da Informação – Ambiente Windows Pleno	Microsoft MCSA – Microsoft Certified Solutions Associate ou Microsoft Certified System Administrator	02
Consultor em Tecnologia da Informação – Ambiente Windows Sênior	Microsoft MCSE – Microsoft Certified Solutions Expert ou Microsoft Certified System Engineer	02
Consultor em Tecnologia da	CompTIA Linux+ ou	02

Perfil do Profissional	Certificação	Quantidade mínima de profissionais certificados
Informação – Ambiente Linux Junior	LPIC Nível I	
Consultor em Tecnologia da Informação – Ambiente Linux Pleno	LPIC Nível II	02
Consultor em Tecnologia da Informação – Ambiente Linux Sênior	LPIC Nível III	01
Gerente de Projetos	PMP - Project Management Professional	01
Analista de Suporte Firewall UTM	Certificação Técnica na Solução de Firewall UTM emitida pelo Fabricante	02
Analista de Suporte Rede Wireless Segura	Certificação Técnica na Solução de Rede Wireless Segura	01

Tabela 1 - Tabela de profissionais certificados

5.3.6. Para efeito de contratação, **a empresa deverá comprovar que possui técnicos com os certificados especificados na Tabela 1**, apresentando cópia autenticada dos certificados dos profissionais ou informações on-line nos sites dos certificadores que possam comprovar a existência das requeridas certificações e atendendo concomitantemente aos itens 5.3.6.1 e 5.3.6.2 logo abaixo:

5.3.6.1. Comprovação de que o profissional é funcionário em regime CLT ou sócio, fornecendo cópia da carteira de trabalho e comprovante de pagamento da GPS do mês anterior ao edital e/ou Contrato/Estatuto Social da Empresa no caso de sócio.

5.3.6.2. O mesmo profissional poderá assumir no máximo 5 (cinco) perfis distintos na tabela de profissionais certificados descritos no item 5.3.5 mais acima.

5.4. Experiência da Licitante Vencedora

5.4.1. Licitante Vencedora deve possuir e apresentar documentação comprobatória já na fase de habilitação referente a Atestados de Capacidade Técnica na/ para a Prestação de Serviços Gerenciados de Segurança da Informação que contemple todas as soluções especificadas neste edital, conferidos por 2 (duas) empresas públicas e/ ou privadas para cada solução contemplada e ainda compatíveis em características, quantidade e tempo de contratação com o objeto da licitação e para atendimento a lista enumerada a partir do item 5.4.1.1 até o item 5.4.1.4 inclusive e abaixo enumeradas:

5.4.1.1. Solução de Firewall UTM

5.4.1.2. Serviço de Wireless Segura.

5.4.1.3. Serviço de Backup.

5.4.1.4. Serviço de Filtro de Conteúdo Web.

5.5. Proibição aos Licitantes

5.5.1. Não será permitida a participação de consórcios de empresas e nem tampouco sublocação de serviços de forma/ modalidade parcial ou total.

6. DESCRIÇÃO DOS NÍVEIS DE SERVIÇOS REQUERIDOS

6.1 Para os serviços de Firewall UTM, Rede Wireless Seguro, Solução de Backup, Solução de correlacionamento de Eventos e Filtro de Conteúdo Web, que fazem parte do objeto deste Termo de Referência, deverão ter/obter/cumprir com:

6.1.1 Disponibilidade de serviço mensal de no mínimo de 99,8% (noventa e nove, vírgula oito por cento). Este percentual será calculado da seguinte forma:

6.1.1.1 Apura-se o número de horas de indisponibilidade no mês.

6.1.1.2 Apura-se o número de horas de disponibilidade do mês.

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

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

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

6.1.1.6 Disponibilidade de serviço anual de, no mínimo de 99,1% (noventa e nove, vírgula um por cento). Este percentual será calculado da seguinte forma:

6.1.1.7 Apura-se o número de horas de indisponibilidade no ano.

6.1.1.8 Apura-se o número de horas de disponibilidade no ano.

6.1.1.9 Subtrai-se o número de horas de disponibilidade no ano pelo número de horas de indisponibilidade no ano.

6.1.1.10 Divide-se o valor obtido no item anterior pelo número de horas de disponibilidade no ano.

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

6.1.1.12 Não serão consideradas indisponibilidade as seguintes situações:

6.1.1.13 Falta de energia no local de instalação das soluções.

6.1.1.14 Indisponibilidade da rede lógica à qual esteja instalado os equipamentos das soluções.

6.1.1.15 Manutenções programadas pela Contratada ou SINE-IDT/CE, com o aceite dado em documento pela parte requerida.

6.2. 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) salvo por fatos plenamente justificáveis e aceitos pelo SINE-IDT/CE.

6.3. Todos os serviços cujos SLA (Acordo de Nível de Serviço) fazem parte do objeto deste Termo de Referência deverão ter disponibilidade de serviço mensal de, no mínimo, 98% (noventa e oito por cento). Este percentual será calculado, por serviço, da seguinte forma:

6.3.1 Apura-se o número de chamados de serviço atendidos dentro do SLA no mês.

6.3.2 Apura-se o número de chamados de serviço atendidos fora do SLA no mês.

6.3.3 Subtrai-se o número de chamados do serviço atendidos dentro do SLA no mês pelo número de chamados de serviços atendidos fora do SLA no mês.

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

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

7 ESPECIFICAÇAO DAS SOLUÇÕES TÉCNICAS - REQUISITOS MÍNIMOS

7.1 Solução de Firewall UTM

7.1.1 Composição da Solução:

7.1.1.1 A solução de Firewall UTM a ser contratada é composta do fornecimento de equipamentos (especificados no item 7.1.3 e 7.1.4) bem como serviços (especificação no item 7.1.2), suporte técnico e manutenção associados a tais equipamentos de acordo com SLA definido no item 7.

7.1.1.2 Nos itens que devem suportar alta disponibilidade (cluster), a solução deverá ser dimensionada de forma que cada equipamento consiga atender na totalidade todas as exigências do edital, não sendo aceitos problemas de performance caso um dos equipamentos falhe.

7.1.2 Serviços a serem desempenhados pela CONTRATADA:

7.1.2.1 O serviço de acompanhamento/implementação de segurança deve ser prestado de forma a atender todas as necessidades do SINE-IDT/CE em implementar e manter as políticas de segurança e deve contemplar:

a) Acompanhamento/implementação de VPN: criação de túneis de VPN para suprir a necessidade de clientes/sites remotos através de uma infraestrutura de rede pública (Internet).

b) Acompanhamento/implementação de Usuários: manutenção de usuários e grupos (criação, alteração e exclusão), definição de políticas de acesso e monitoração do acesso.

c) Acompanhamento/implementação da Operação: backup de configuração de sistemas (regras), aplicação de "Patches" e novas atualizações de software, gerenciamento de modificações e análise de logs.

d) Monitoração dos firewalls: alertas de invasões, análise de tráfego atípico, detecção de "Scans", Spoofing, tentativas de autenticações sem permissão, dentre outras correlatas.

e) Acompanhamento/implementação de Antivírus: Monitoração constante da presença de vírus através do firewall.

f) Manutenção dos Firewalls: Compreende a atualização de software para o perfeito funcionamento do dispositivo.

g) Detecção de ataques de rede: Monitoração constante de ataques ou tentativa de invasão de redes, incluindo "Port Scan", "Denial of Services - DOS", e ataques de autenticação, notificando a equipe do SINE-IDT/CE tomando as ações corretivas necessárias.

h) A Contratada será responsável, sem ônus adicional ao SINE-IDT/CE por ministrar treinamento para até 7 (sete) pessoas pertencentes ao quadro funcional da Contratante na solução de Firewall UTM através de centro de treinamento e instrutor oficial, ficando facultado a aplicação do exame oficial para certificação em Centro de Certificação Oficial, também sem ônus adicional.

7.1.2.2 Relatórios e seus requisitos mínimos: O serviço de acompanhamento/implementação deve permitir o acesso seguro, via portal disponível na Plataforma de Acompanhamento, aos seguintes tipos de relatórios:

a) Relatório de Utilização de Banda.

b) Relatório de Utilização WEB.

c) Relatório de Filtragem WEB.

d) Relatório de Utilização FTP.

e) Relatório de Utilização de E-mail.

f) Relatório de Utilização de VPN.

g) Relatório de Ataques.

7.1.2.3 Relatórios de Funcionalidade e ações das soluções: O SINE-IDT/CE poderá solicitar, sempre que julgar necessário, relatórios que demonstrem o funcionamento das soluções.

7.1.2.4 Plataforma de Acompanhamento e seus requisitos mínimos: A Contratada deverá ter o seu SNOC (Security and Network Operation Center) equipado com uma Plataforma de Acompanhamento que permita atender prontamente a todas as requisições do SINE-IDT/CE para as previsibilidades/necessidades de configurações, acompanhamento/implementação e o monitoramento de "Firewalls" e de serviços de VPN IPSec, Antivírus e IPS através da mesma interface (única plataforma de software) e capaz de oferecer ao SINE-IDT/CE o acesso remoto a esta interface. Também de forma a permitir o controle e a visualização de todos os parâmetros e funcionalidades gerenciadas com as demais seguintes características:

a) Permitir não só a configuração, como também o acompanhamento/implementação centralizados capaz de possibilitar aos administradores de rede, de forma global, definir, distribuir, forçar e implementar um amplo número de serviços, atualizações e políticas de segurança para os "Firewalls" gerenciados.

b) Permitir o fornecimento de um conjunto adicional de privilégios para operadores de gerencia de segurança e a outros operadores não administradores.

c) Permitir a visão do status atual dos "Firewalls", tarefas pendentes e mensagens de "LOG", além dos relatórios gráficos dos "Firewalls" e atividades da rede por "Firewall".

d) Prover relatórios gráficos das atividades dos "Firewalls" bem como do uso de banda e de eventos de segurança tais como ataques.

e) Possuir visualizador integrado de "LOGS" em tempo real.

f) Permitir a visualização dos relatórios através das interfaces gráficas da plataforma de Acompanhamento via sessões Web HTTP e HTTPS.

g) Possibilitar o exame e auditoria das atividades dos administradores e operadores do ambiente de gerenciamento.

h) Possibilitar o envio de alertas e notificações por e-mail ao administrador de segurança.

i) Permitir o monitoramento em tempo real de elementos de rede através do estado up/down e da latência de uma porta TCP/IP.

j) Permitir a visualização de relatórios percentuais do tempo (SLA) que o firewall está up/down desde a sua primeira instalação.

7.1.2.5 Avaliação da Configuração e Melhoria Contínua:

7.1.2.6 A Contratada ficará responsável pela aplicação das recomendações de segurança, atualizações e de melhorias conforme recomendações exaradas pelo fabricante da solução em utilização.

7.1.2.6.1 A Contratada deverá comunicar ao SINE-IDT/CE sempre que surgir uma nova versão de software das soluções, dando parecer quanto às suas instalações e cronograma, possíveis impactos e auxiliando na decisão quanto ao melhor momento para a aplicação das melhorias.

7.1.3. Outros Requisitos Gerais Mínimos:

7.1.2.7 Todos os equipamentos de Firewall UTM deverão atender aos requisitos mínimos de funcionalidades tais como as abaixo elencadas:

7.1.2.8 Solução em *appliance* de *firewall stateful packet inspection* com capacidade de *deep packet inspection* para filtragem de tráfego IP. Não serão aceitas soluções baseadas em PC de uso geral ou soluções que contenham componentes do tipo acionadores de discos rígidos ou flexíveis.

7.1.2.9 Não serão aceitas soluções que tenham limitação quanto ao tamanho de arquivo inspecionado pelo appliance.

7.1.2.10 Fornecimento de suporte a VPN IPSec, incluindo criptografia DES-56 bits, 3DES-168 bits, AES-128, AES-192 e AES-256, com capacidade de implementar topologias site-to-site e client-to-site.

7.1.2.11 Implementar recurso de NAT (Network Address Translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, e tradução simultânea de endereço IP, porta TCP de conexão (NAPT), e NAT transversal em VPN IPSec.

7.1.2.12 Possuir servidor de DHCP (dynamic host configuration protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e em VPN e detecção de duplicação de endereços.

7.1.2.13 Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

7.1.2.14 Possuir mecanismo que limite o número máximo de conexões simultâneas de uma mesma origem a um determinado serviço ou a um determinado servidor e que possa ser aplicado individualmente para cada regra de filtragem.

7.1.2.15 Possuir validação completa da sintaxe de toda sinalização de VoIP e pacotes de streams de mídia (para assegurar que pacotes malformados não possam passar pelo firewall e afetar adversamente o destinatário da comunicação).

7.1.2.16 Possuir suporte à configuração dinâmica e rastreamento de cada chamada de VoIP.

7.1.2.17 Suportar o registro do firewall dinamicamente, pelo seu endereço IP de WAN, num provedor de serviços de DDNS.

7.1.2.18 Suportar endereçamento na interface de WAN por PPPOE (Point-to-point Protocol Over Ethernet), IP estático e dinâmico, por DHCP e PPTP (point-to-point tunneling protocol).

7.1.2.19 Permitir alta disponibilidade das interfaces WAN nas modalidades ativo-ativo (balanceamento) e ativo-passivo (redundância).

7.1.2.20 Possuir capacidade de definição de múltiplas regiões de segurança no firewall, com objetos e regras de acesso distintas, de modo que o administrador possa definir interfaces e com características específicas, em regiões ou zonas lógicas do firewall.

7.1.2.21 Permitir a definição de objetos como grupo de usuários, redes ou serviços de modo que, quando a política de segurança mudar, o administrador possa modificar o objeto pré-definido e propagar as mudanças instantaneamente sem necessidade de redefinir as regras.

7.1.2.22 Possuir gerenciamento de banda de entrada e saída, suporte 802.1p e classes de serviço por DSCP (differentiated services code points).

7.1.2.23 Possuir recurso de balanceamento de links WAN, com regras de balanceamento por conexão utilizando a métrica round-robin, e funcionalidade de escoamento de tráfego para a interface WAN secundária, quantificável em kbps e percentual de utilização para cada interface WAN de dados.

7.1.2.24 Possuir mecanismo que possibilite o funcionamento transparente dos protocolos FTP, Real Audio, Real Video, SIP, RTSP e H.323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro.

7.1.2.25 Possuir suporte ao protocolo SNMP, através de MIB2.

7.1.2.26 Condições Mínimas de Autenticação:

7.1.2.26.1 Prover autenticação de usuários para os serviços TELNET, FTP, HTTP e HTTPS de forma simultânea.

7.1.2.26.2 Permitir a autenticação dos usuários utilizando servidores LDAP, AD e RADIUS.

7.1.2.26.3 Permitir o cadastro manual dos usuários e grupos diretamente no firewall por meio da interface de gerência remota do equipamento.

7.1.2.26.4 Permitir a integração com qualquer autoridade certificadora emissora de certificados X. 509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando certificados revogados emitidos periodicamente pelas autoridades.

7.1.2.26.5 Permitir o controle de acesso por usuário, para plataformas Microsoft Windows 2000 e Microsoft Windows XP de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

7.1.2.26.6 Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

7.1.2.26.7 Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

7.1.2.26.8 Suportar padrão IPSec, de acordo com as RFC 2401 a 2412, de modo a estabelecer canais de criptografia com outros produtos que também suportem tal padrão.

7.1.2.26.9 Suportar a criação de túneis seguros sobre IP (IPSec tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

7.1.2.27 Administração:

7.1.2.27.1 A interface gráfica deverá possuir assistentes para facilitar a configuração inicial e administração do firewall, incluindo a configuração de VPNs e NATs.

7.1.2.27.2 Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o firewall, com no mínimo dois níveis de permissão: total e apenas leitura.

7.1.2.27.3 Permitir a conexão simultânea de vários administradores, concedendo o uso de permissão total apenas para o primeiro administrador autenticado com este nível de permissão. Aos demais, independentemente de seu perfil, será concedida apenas permissão de leitura. O firewall deverá permitir que o segundo administrador com permissão total envie mensagem ao primeiro administrador a se autenticar com permissão total.

7.1.2.27.4 Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o firewall.

7.1.2.27.5 Possuir mecanismo para realizar remotamente, pela interface gráfica, cópias de segurança (backup) e restauração, sem a necessidade de se reinicializar o sistema (no caso de realização de backups).

7.1.2.27.6 Permitir a visualização e o gerenciamento em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do firewall, por serviços e endereços IP de origem e destino.

7.1.2.27.7 Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do firewall, em tempo real.

7.1.2.27.8 Permitir a visualização em tempo real, dos serviços com maior tráfego e os endereços IPs mais acessados.

7.1.2.27.9 Possibilitar o controle do tráfego, pelos endereços de origem e destino da comunicação.

7.1.2.27.10 Possuir suporte a roteamento RIP e OSPF.

7.1.2.27.11 Possuir interface orientada a linha de comando para a administração do firewall a partir do console ou conexão SSH.

7.1.2.28 LOG:

7.1.2.28.1 Possuir suporte a LOG via Syslog.

7.1.2.28.2 Possibilitar o registro da comunicação realizada através do firewall, sob demanda do administrador, das conexões abertas e das conexões recusadas pelo mesmo.

7.1.2.28.3 Prover mecanismo (s) de consulta às informações registradas e integradas à interface de administração.

7.1.2.28.4 Possibilitar a análise dos seus registros (LOGs) por pelo menos um programa analisador de LOG disponível no mercado.

7.1.2.28.5 Possuir mecanismo que permita inspecionar o tráfego de rede em tempo real (sniffer) via interface gráfica, possibilitando exportar os dados visualizados para arquivo formato PCAP e permitindo a filtragem dos pacotes por protocolo, endereço IP de origem, endereço IP de destino, porta TCP de origem e porta TCP de destino.

7.1.2.28.6 Permitir a visualização do tráfego de rede em tempo real tanto nas interfaces de rede do firewall quando nos pontos internos do mesmo: anterior e posterior à filtragem de pacotes, onde o efeito do NAT é eliminado.

7.1.2.28.7 Não serão aceitas soluções baseadas em redirecionamento de tráfego para dispositivos externos ao firewall para análise de arquivos ou pacotes de dados.

7.1.2.29 Voltagem Elétrica e Frequência:

7.1.2.29.1 Possuir fonte de alimentação operando nas tensões 110/220V, com seleção automática de voltagem, e frequência de 50/60Hz.

7.1.2.30 Entrega dos Equipamentos:

7.1.2.30.1 Todos os equipamentos aqui considerados como tratando-se de appliances que deverão ser objeto de entrega na condição de novos e sem uso prévio, devendo também e obrigatoriamente estar em linha de produção, sem previsão de descontinuidade até a data da proposta de preços.

7.1.3 Requisitos Específicos Mínimos para os Tipos de **Soluções de Firewall UTM:**

7.1.3.1 Serviço de Firewall UTM e aqui denominado Médio e Grande Porte – Tipo I:

7.1.3.1.1 Possuir, no próprio *firewall*, recursos de filtro de conteúdo e de inspeção, por técnica DPI, de antivírus e *antispyware* de *gateway* e IPS, a fim de detectar e prevenir a ocorrência de *spyware*, vírus, *trojans* e *worms*, intrusões, vulnerabilidades de protocolos, sistemas operacionais e aplicativos de servidores, nos protocolos SMTP, POP3, IMAP, HTTP, FTP, NETBIOS e TCP STREAM, através de assinaturas, em tempo real, sem a utilização de proxies e com tamanho de arquivo ilimitado e quantidade de *downloads* simultâneos em número igual ao de conexões suportadas pelo equipamento.

7.1.3.1.2 Ser capaz de atualizar automaticamente as assinaturas de vírus e spyware e IPS sem a necessidade de intervenção humana.

7.1.3.1.3 Possuir recursos capazes de detectar e evitar automaticamente IP source spoofing, IP source routing, túnel IPSec e ataques tipo DoS (denial-of-service) como Ping of Death, SYN flood, land attack e IP spoofing, com a possibilidade de atualizar as assinaturas e de carregar as novas através da atualização do software de sistema operacional do equipamento.

7.1.3.1.4 Deve permitir a utilização de regras de antivírus, antispyware, IDS e IPS e filtro de conteúdo por segmentos de rede e/ou por VLANs, quando o equipamento suportar VLAN's. Todos os serviços devem ser suportados no mesmo segmento de rede ou VLAN.

7.1.3.1.5 Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de pelo menos 6 (seis) softwares p2p (peer-to-peer) incluindo Kazaa, Limewire, Morpheus e Napster e de pelo menos 6 (seis) comunicadores instantâneos (Instant Messengers), incluindo ICQ, MSN (incluindo sua nova versão, o Windows Live, da Microsoft), Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

7.1.3.1.6 Ser capaz de detectar e bloquear no mínimo 2.000 (duas mil) assinaturas diferentes de Malware.

7.1.3.1.7 Possuir a funcionalidade de hardware-failover ativo/passivo.

7.1.3.1.8 Controle de conteúdo Web

7.1.3.1.8.1 .Possuir módulo de filtro de conteúdo integrado ao firewall para classificação de páginas web com no mínimo 50 (cinquenta) categorias distintas, com mecanismo de atualização automática.

7.1.3.1.8.2 .Controle de conteúdo por categorias de filtragem com base de dados diariamente atualizada pelo fabricante.

7.1.3.1.8.3 Permitir que o SINE-IDT/CE possa vir a ter prerrogativa de solicitar, via web, a classificação ou reclassificação de sites na base de categorias do fabricante.

7.1.3.1.8.4 Permitir a classificação dinâmica de sites web, URLs e domínios.

7.1.3.1.8.5 Suportar a filtragem de conteúdo sobre os seguintes assuntos, no mínimo (o nome da categoria pode variar de acordo com o fabricante, mas o conteúdo a ser bloqueado deve ser o mesmo):

7.1.3.1.8.5.1 . Violência.

7.1.3.1.8.5.2 Nudismo.

7.1.3.1.8.5.3 Pornografia.

7.1.3.1.8.5.4 Armas.

7.1.3.1.8.5.5 Racismo.

7.1.3.1.8.5.6 Drogas ilegais.

7.1.3.1.8.5.7 Crimes.

7.1.3.1.8.5.8 Comportamento ilegal.

7.1.3.1.8.5.9 Jogos.

7.1.3.1.8.5.10 Álcool.

7.1.3.1.8.5.11 Tabagismo.

7.1.3.1.8.5.12 Conteúdo adulto.

7.1.3.1.8.5.13 Entretenimento.

7.1.3.1.8.5.14 Chat.

7.1.3.1.8.5.15 WebMail.

7.1.3.1.8.5.16 Jogos de azar.

7.1.3.1.8.5.17 Navegação anônima.

7.1.3.1.8.5.18 Humor.

7.1.3.1.8.5.19 Newsgroups.

7.1.3.1.8.5.20 Encontros pessoais.

7.1.3.1.8.5.21 Streaming de músicas e vídeos.

7.1.3.1.8.5.22 Download de software.

7.1.3.1.8.6 Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

7.1.3.1.8.7 Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de Web.

7.1.3.1.8.8 Possibilitar a filtragem da linguagem Java script e de applets Java e Active-x em páginas WWW, para o protocolo HTTP.

7.1.3.1.8.9 Equipamento deve suportar mecanismo de alta-disponibilidade do Firewall através da adição de unidades secundárias (HA).

7.1.3.1.8.10 Possuir, no mínimo, 12 (doze) interfaces Gigabit 10/100/1000.

7.1.3.1.8.11 Possuir, no mínimo, 2 (duas) interfaces 10GbE SFP+ com transceivers fornecidos.

7.1.3.1.8.12 Possuir, no mínimo, 1 interface padrão USB.

7.1.3.1.8.13 Suportar no mínimo:

7.1.3.1.8.13.1 39.000 (trinta e nove mil) usuários autenticados simultaneamente.

7.1.3.1.8.13.2 322.000 (trezentas e vinte e duas mil) conexões TCP/IP simultâneas no modo firewall.

7.1.3.1.8.13.3 800 (oitocentos) túneis VPN site-to-site e suportar 1.000 (mil) túneis VPN client-to-site simultâneos, licenciado para no mínimo 50 (cinquenta) conexões.

7.1.3.1.8.13.4 20.000 (vinte mil) novas conexões por segundo.

7.1.3.1.8.14 Possuir performance de:

7.1.3.1.8.14.1 Firewall stateful inspection de no mínimo 3,4 Gbps (três gigabits e quatrocentos megabits por segundo).

7.1.3.1.8.14.2 Antivírus de Gateway de no mínimo 600 Mbps (seiscentos megabits por segundo).

7.1.3.1.8.14.3 UTM (combinação de todas as funcionalidades habilitadas) de no mínimo 900 Mbps (novecentos megabits por segundo).

7.1.3.1.8.14.4 IPS de no mínimo 1.1 Gbps (um gigabit e cem megabits por segundo).

7.1.3.1.8.14.5 VPN IPSec (3DES/AES) de no mínimo 1.5 Gbps (um gigabit e quinhentos megabits por segundo).

7.1.5. Serviço de Firewall UTM aqui denominado de Pequeno Porte – Tipo II:

7.1.5.1. Possuir, no mínimo, 5 (cinco) interfaces Gigabit 10/100/1000.

7.1.5.1.1.Possuir, no mínimo, 1 interface padrão USB.

7.1.5.1.2. Suportar:

7.1.5.1.1.1. 250 (duzentos e cinquenta) usuários autenticados simultaneamente.

7.1.5.1.1.2. 10.000 (dez mil) conexões TCP/IP simultâneas no modo firewall.

7.1.5.1.1.2. 10 (dez) túneis VPN site-to-site e suportar 5 (cinco) túneis VPN client-to-site simultâneos, licenciado para no mínimo 1 (uma) conexão.

7.1.5.1.3. 800 (mil e oitocentas) novas conexões por segundo.

7.1.5.1.3. Possuir performance:

7.1.5.1.3.1. Firewall stateful inspection de no mínimo 300 Mbps (trezentos megabits por segundo).

7.1.5.1.3.2. Antivírus de Gateway de no mínimo 50 Mbps (cinquenta megabits por segundo).

7.1.5.1.3.3. UTM (combinação de todas as funcionalidades habilitadas) de no mínimo 60 Mbps (sessenta megabits por segundo).

7.1.5.1.3.4. IPS de no mínimo 100 Mbps (cem megabits por segundo).

7.1.5.1.3.5. VPN IPSec (3DES/AES) de no mínimo 100 Mbps (cem megabits por segundo).

7.2 Serviço de Rede Wireless Segura

7.2.1 Composição da Solução:

7.2.1.1 A solução de Rede Wireless contratada é composta do fornecimento de equipamentos, bem como serviços, suporte técnico e manutenção associada a tais equipamentos (de acordo com SLA definido no item 7).

7.2.2 Serviços Requeridos:

7.2.2.1 Relatórios de Funcionalidade e ações da solução: A Licitante poderá solicitar, sempre que julgar necessário, relatórios que demonstrem o funcionamento das soluções.

7.2.2.2 Gráficos em tempo real e com registro histórico de características da solução, permitindo visualizar para todos os componentes da solução:

7.2.2.2.1.1 Utilização de CPU e memória.

7.2.2.2.1.2 Utilização de largura de banda das interfaces de rede.

7.2.2.2.1.3 Disponibilidade de cada componente da solução, medido através de pooling SNMP ou PING.

7.2.2.3 O serviço de acompanhamento/implementação de segurança deve ser prestado de forma a atender todas as necessidades do SINE-IDT/CE em implementar e manter as políticas de segurança.

7.2.2.4 Avaliação da Configuração e Melhoria Contínua

7.2.2.4.1 A Licitante ficará responsável pela aplicação das recomendações de segurança, atualizações e melhorias conforme recomendações do fabricante da solução.

7.2.2.4.1.1 A Licitante deverá comunicar ao SINE-IDT/CE sempre que surgir uma nova versão de softwares das soluções, dando parecer quanto as suas instalações e cronograma, possíveis impactos e auxiliando na decisão quanto ao melhor momento para a aplicação das melhorias.

7.2.3 Wireless Access Point

7.2.3.1 Composição da Solução:

7.2.3.1.1 A solução de Rede Wireless – Wireless Access Points contratada é composta do fornecimento de equipamentos, bem como serviços, suporte técnico e manutenção associada a tais equipamentos (de acordo com SLA definido no item 7).

7.2.3.2 Deve Implementar funcionamento em modo gerenciado através de controladora e auto gerenciado, sem necessidade de controladora WLAN para configuração de seus parâmetros de rede wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF. O AP poderá está configurado em um modo gerenciado e depois ser reconfigurado para o modo não gerenciado e vice-versa. Deve obedecer à todas as características descritas mesmo neste modo de funcionamento.

7.2.3.3 No modo de funcionamento auto gerenciado, deve permitir a formação de conjuntos de pontos de acesso que se comuniquem e compartilhem das mesmas configurações (Clusters).

7.2.3.4 No modo de funcionamento auto gerenciado, deve disponibilizar uma interface gráfica única e centralizada, acessível por browser padrão em página https, para configuração do conjunto de Pontos de Acesso (cluster).

7.2.3.5 A solução em modo auto gerenciado deve ser redundante dentro do cluster e não deve depender única e exclusivamente de um elemento do cluster, ou seja, em caso de falha de um ou mais pontos de acesso a solução deve continuar funcionando, mesmo que só com um ponto de acesso.

7.2.3.6 Equipamentos e seus Requisitos Mínimos:

7.2.3.6.1 Cada Access Point deve ser fornecido juntamente com 01 (um) Injetor PoE compatível com a tecnologia 802.3af.

7.2.3.6.2 Equipamento de Ponto de Acesso para rede local sem fio, configurável via software, com funcionamento simultâneo nos padrões IEEE 802.11a/n, 5GHz, e IEEE 802.11b/g/n, 2.4GHz.

7.2.3.6.3 Deve ser capaz funcionar em modo gerenciado por controlador WLAN, para configuração de seus parâmetros wireless, gerenciamento das políticas de segurança, QoS e monitoramento de RF.

7.2.3.6.4 Deve ser capaz de trabalhar com controladores WLAN em redundância.

7.2.3.6.5 Deve permitir usuários configurados nos padrões IEEE 802.11b/g/n e 802.11a/n simultaneamente.

7.2.3.6.6 Deve ser capaz de implementar as seguintes taxas de transmissão e com fallback automático.

7.2.3.6.6.1 IEEE 802.11 a/g: 54, 48, 36, 24, 18, 12, 9 e 6 Mbps.

7.2.3.6.6.2 IEEE 802.11 b: 11; 5,5; 2 e 1 Mbps.

7.2.3.6.6.3 IEEE 802.11n: MCS0 - MSC15 (6.5Mbps - 300Mbps).

7.2.3.6.7 Implementar o protocolo de enlace CSMA/CA para acesso ao meio de transmissão.

7.2.3.6.8 Operar nas modulações DSSS, OFDM e 802.11n (2X2 MIMO) com dois spatial streams.

7.2.3.6.9 Possuir capacidade de selecionar automaticamente o canal de transmissão.

7.2.3.6.10 Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF.

7.2.3.6.11 Possuir suporte a pelo menos 32 SSIDs.

7.2.3.6.12 Permitir habilitar e desabilitar a divulgação do SSID.

7.2.3.6.13 Implementar diferentes tipos de combinações criptografia/autenticação por SSID.

7.2.3.6.14 Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras, possuindo certificação.

7.2.3.6.15 Não deve haver licença restringindo o número de usuários por ponto de acesso.

7.2.3.6.16 Possuir antenas compatíveis com as frequências de rádio dos padrões IEEE 802.11a/n e 802.11/b/g/n com ganho de, pelo menos, 4 dBi e 3.9 dBi, respectivamente, com padrão de irradiação omnidirecional multi-banda dipolar, integral e dual (2X2 MIMO com diversidade espacial).

7.2.3.6.17 Possuir potência máxima de transmissão de, no mínimo, 21 dBm para IEEE 802.11a/b/g/n.

7.2.3.6.18 Deve possuir sensibilidade de recepção de valor menor ou igual: a -96 dBm a 6Mbps no padrão 802.11g/n; e a -96 dBm a 6Mbps no padrão 802.11a/n.

7.2.3.6.19 Implementar a pilha de protocolos TCP/IP.

7.2.3.6.20 Implementar VLANs conforme padrão IEEE 802.1Q.

7.2.3.6.21 Possuir, no mínimo, uma interface IEEE 802.3 10/100/1000Base Ethernet, auto-sensing, auto MDI/MDX, com conectores RJ-45, para conexão à rede local fixa.

7.2.3.6.22 Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono).

7.2.3.6.23 Implementar cliente DHCP, para configuração automática de rede.

7.2.3.6.24 Deve configurar-se automaticamente ao ser conectado na rede.

7.2.3.6.25 Possuir LED's indicativos do estado de operação, da atividade do rádio e da interface Ethernet.

7.2.3.6.26 Possibilitar alimentação elétrica local e via padrão PoE (IEEE 802.3af).

7.2.3.6.27 Possuir estrutura que permita fixação do equipamento em teto e parede e fornecer acessórios para que possa ser feita a fixação.

7.2.3.6.28 Implementar varredura de RF nas bandas 802.11a, 802.11b, 802.11g e 802.11n para identificação de Pontos de Acesso intrusos não autorizados (rogues) e interferências no canal habilitado ao ponto de acesso e nos demais canais configurados na rede WLAN, sem impacto no seu desempenho.

7.2.3.6.29 Possibilitar emprego de tecnologia mesh.

7.2.3.6.30 A potência de transmissão deve permitir ajuste em intervalos de 0,5 dBm.

7.2.3.6.31 Deve ser capaz de implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-MD5, EAP-FAST, EAP-TLS, PEAP-GTC, PEAP-MSCHAPv2.

7.2.3.6.32 Suportar a autenticação com geração dinâmica de chaves criptográficas por sessão e por usuário.

7.2.3.6.33 Deve ser capaz de implementar WPA com algoritmo de criptografia TKIP e MIC.

7.2.3.6.34 Deve ser capaz de implementar WPA2 com algoritmo de criptografia AES, IEEE 802.11i.

7.2.3.6.35 Deve ser capaz de implementar função de análise de espectro nas frequências de 2.4 e 5 GHz, identificando origens de interferências, sejam elas 802.11 ou outras.

7.2.3.6.36 Possuir módulo TPM (Trusted Platform Module) integrado, criptoprocessador seguro, para proteger as informações através de chaves criptográficas.

7.2.3.6.37 Possuir Certificação de Homologação junto a ANATEL.

7.2.4 Software de Gerência Rede Wireless Segura

7.2.4.1 O software de gerência deverá ser fornecido em appliance físico ou virtual.

7.2.4.2 Deve ser obrigatoriamente do mesmo fabricante dos pontos de acesso e controladores;

7.2.4.3 Permitir a configuração e gerenciamento através de browser padrão (http, https);

7.2.4.4 Deve ser capaz de gerenciar todos os APs e controladores WLAN constantes nesse documento;

7.2.4.5 Permitir que os eventos sejam gravados remotamente utilizando Syslog;

7.2.4.6 Prover organização hierárquica de equipamentos, permitindo que um equipamento receba as configurações lógicas e as replique a outros equipamentos.

7.2.4.7 Possuir capacidade de projeto automatizado de redes sem fio nos padrões 802.11a, 802.11b e 802.11g, 802.11n e 802.11ac, segundo a geografia do prédio (planta).

7.2.4.8 Considerar a área de cobertura e a banda por usuário desejada;

7.2.4.9 Possibilitar a importação de plantas baixas nos formatos dwg e jpg;

7.2.4.10 Permitir a visualização de alertas da rede em tempo real.

7.2.4.11 Permitir a visualização de eventuais áreas sem cobertura de RF (áreas de sombra);

7.2.4.12 Monitorar o desempenho da rede wireless, consolidando informações de rede tais como: níveis de ruído, relação sinal-ruído, interferência, potência de sinal.

7.2.4.13 Possuir capacidade de listagem on-line da localização de usuário, endereço IP, endereço MAC, nível de potência de recepção e dados de associação e de autenticação 802.1x.

7.2.4.14 Deve possuir informação visual e gráfica, planta baixa dos andares, para:

7.2.4.14.1 Visualização dos Aps instalados, com estado de funcionamento.

7.2.4.14.2 Visualização do mapa de calor de RF (Heatmap).

7.2.4.14.3 Localização de ativos conectados à rede (equipamentos 802.11).

7.2.4.14.4 Localização de rogue Aps.

7.2.4.14.5 Caso esta funcionalidade não esteja disponível no sistema de gerência, deve ser fornecido software, do mesmo fabricante, para atender este item, contemplando toda a rede e com redundância 1+1.

7.2.4.15 Possuir capacidade de identificação e listagem dos rádios vizinhos e respectivos SSID/BSSID que podem ser percebidos por cada AP,

7.2.4.16 Possuir capacidade de configuração gráfica completa do Controlador WLAN e respectivos APs.

7.2.4.17 Suportar SSH, HTTP/HTTPS, **SSL**, Telnet.

7.2.4.18 Possuir ferramentas de debug e log de eventos para depuração e gerenciamento em primeiro nível.

7.2.4.19 Implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

7.2.4.20 Possuir suporte a MIB II, conforme RFC 1213;

7.2.4.21 Implementar a MIB privativa que forneça informações relativas ao funcionamento do equipamento.

7.2.4.22 Possibilitar a obtenção da configuração do equipamento através do protocolo SNMP.

7.2.4.23 Possibilitar a obtenção via SNMP de informações de capacidade e desempenho da CPU, memória e portas.

7.2.4.24 Possibilitar a gerência e identificação individualizada de cada AP remoto.

7.2.4.25 Permitir a administração centralizada dos APs sem a necessidade de configurar os APs individualmente.

7.2.4.26 Possibilitar a identificação de paredes e divisórias com respectivos níveis de atenuação por tipo (alvenaria, vidro, drywall e divisória).

7.2.4.27 Possibilitar a importação de plantas baixas nos formatos gráficos (CAD, dwg, jpg, gif e png);

7.2.4.28 Deve disponibilizar em painel gráfico de controle informações referentes à:

7.2.4.28.1 Sistemas operacionais e tipos de dispositivos que estão se conectando a rede.

7.2.4.28.2 Informações sobre chamadas de voz, seus protocolos e qualidade das mesmas.

7.2.4.28.3 Informações sobre os tipos de aplicações mais utilizados.

7.2.4.28.4 Informações sobre usuários conectados.

7.2.4.29 Deve possuir informação sobre possíveis ameaças a rede detectadas pelos sistemas gerenciados.

7.2.4.30 Deve possibilitar criação de regras de detecção de ameaças e correlacionar todos os dispositivos gerenciados.

7.2.4.31 A solução deverá estar licenciada para no mínimo 50 dispositivos, podendo ser expansível a pelo menos a quantidade de APs aqui registrados.

7.3 Serviço de Backup

7.3.1 Espaço para Backup em Disco de Rede (NAS) Remoto

7.3.2 Deverá ser disponibilizado espaço em disco, com volume mínimo de 10TB, acessível através de rede com link dedicado, ou seja, serviço de Cloud Computing, deve ser possível sua expansão e disponibilização da mesma em 24 horas após necessidade/solicitação do CONTRATANTE, com disponibilidade de tempo integral (24x7x365 - vinte quatro horas por dia, sete dias por semana, todos os dias do ano);

7.3.3 Suportar no mínimo os seguintes protocolos para acesso: CIFS ou SMB;

7.3.4 Para viabilizar a comunicação com baixa latência para restaurações rápidas, a Contratada deverá disponibilizar um link dedicado, estabelecer conectividade privada entre a CONTRATADA e a CONTRATANTE, possibilitando, a redução dos custos de rede e garantindo segurança lógica, o recurso deve ter a opção de ser compartilhado, de forma que nenhum outro cliente da CONTRATADA possa ter acesso aos dados da CONTRATANTE. O link deverá prover alta taxa de transferência de largura de banda com no mínimo 50 Mbps, uma rede mais consistente que baseadas em Internet, de baixa latência com no máximo 10 ms de media;

7.3.5 Não deverá haver cobranças adicionais por download, ou seja, **sem limite de volume de transferências;**

7.3.6 O acesso a esse recurso deverá ser realizado através de um usuário e senha disponibilizado ao SINE – IDT/CE de forma a garantir a segurança dos dados armazenados.

7.4 Serviço de Filtro de Conteúdo Web

7.4.1 Características de Hardware

7.4.1.1 A solução deverá ser fornecida em appliance específico obrigatoriamente do mesmo fabricante (Hardware e Software);

7.4.1.1.1 Não serão aceitas soluções de software embarcadas em hardwares genéricos;

7.4.1.2 A solução deverá ser capaz de aguentar a seguinte volumetria de tráfego:

7.4.1.2.1 Requisições/Segundo HTTP: 700

7.4.1.2.2 Requisições/Segundo HTTPS: 350

7.4.1.2.3 Quantidade de Usuários: 7.000

7.4.1.2.4 Tamanho Cache: 200 Gb

7.4.1.3 A solução deverá compreender, no mínimo:

7.4.1.3.1 01 (um) Servidor Central de Relatórios;

7.4.1.3.2 01 (um) Servidores de Análise de URL;

7.4.1.4 Caso o fabricante possua appliance virtual será aceito o fornecimento do mesmo, desde que obedeça ao requisito mínimo informado;

7.4.1.5 A Solução deve prover aceleração de entrega de conteúdo para usuários;

7.4.1.6 Deve possuir serviço de proxy nativo e integrado ao appliance ofertada para gerenciamento de dados em tempo real, sem a necessidade de caixa adicionais para a realização deste serviço

7.4.2 Características Básicas da Solução

7.4.2.1 A solução proposta deverá implantar a funcionalidade de filtro de URL's HTTP, HTTPS e FTP

7.4.2.2 A solução deverá implantar filtro de Conteúdo HTTP e HTTPS;

7.4.2.3 A solução deverá realizar a verificação de conteúdo e URL em canais criptografados (SSL)

7.4.2.4 A solução deve suportar o protocolo ICAP (Internet Content Adaptation Protocol) para análise de malware;

7.4.2.5 A solução deverá suportar redirecionamento para filtragem via WCCP (Web Cache Communication Protocol);

7.4.2.6 Deverá suportar os seguintes modos de instalação:

7.4.2.6.1 Modo Proxy

7.4.2.6.2 Modo Proxy Reverso

7.4.2.6.3 Modo Proxy High Availability

7.4.2.6.4 Modo Transparente Router

7.4.2.6.5 Modo Transparente Bridge

7.4.2.7 Deverá implantar dois modos de maneira simultânea sem necessidade de reinstalação ou reconfiguração completa da solução, como por exemplo:

7.4.2.7.1 Modo Proxy e Modo Transparente;

7.4.2.8 Caso a solução não possibilite o funcionamento em modo simultaneo dos dois modos solicitados, o fornecedor deverá entregar o ambiente de maneira duplicada;

7.4.2.9 Ao ser configurado em modo transparente bridge o equipamento deverá efetuar a monitoração e proteção de segmentos de rede em modo transparente e operação na camada 2 (Layer-2) do modelo OSI (Open System Interconnection), ou seja, interface de monitoração e proteção não requer endereço IP configurado;

7.4.2.10 A configuração das placas de rede da solução ofertada deve suportar tanto IPv4 como IPv6;

7.4.2.11 Em ambas configurações de IPv4 como IPv6 deve ser possivel a configuração do MTU;

7.4.2.12 A solução deve permitir a configuração manual e/ou automática de horário através de uso NTP configurada na solução;

7.4.2.13 O produto deve possuir proxy proprietários especificos para manuseio de todos protocolos abaixo citados:

7.4.2.13.1 HTTP;

7.4.2.13.2 HTTPS;

7.4.2.13.3 FTP:

7.4.2.13.3.1 Configuração da porta de funcionamento ICAP;

7.4.2.13.3.2 Endereço IP responsável pelo manuseio das conexões ICAP;

7.4.2.13.3.3 Número máximo de conexões concorrentes para REQMOD;

7.4.2.13.3.4 Número máximo de conexões concorrentes para RESPMOD;

7.4.2.13.4 ICAP;

7.4.2.13.4.1 Configuração da porta de funcionamento do proxy FTP;

7.4.2.13.4.2 Endereço IP responsável pelo manuseio das conexões FTP;

7.4.2.13.4.3 Configuração da porta de dados (DATA PORT);

7.4.2.13.4.4 Escopo de portas responsáveis por ouvir os clientes (Port Range for client listener);

7.4.2.13.4.5 Escopo de portas responsáveis por ouvir os servidores (Port Range for server listener);

7.4.2.13.4.6 Permitir ou não os clientes FTP a utilização de modo passivo de FTP;

7.4.2.14 O produto deve possuir função de CACHE nativa na solução sem necessidades de produtos terceiros ou utilização de outros appliances para a realização desta função;

7.4.2.15 Deve possibilitar a configuração dos produtos um tempo de expiração de conexões para os protocolos HTTP(S), FTP e ICAP com os seguintes parametros:

7.4.2.15.1 Timeout para conexão inicial;

7.4.2.15.2 Timeout para conexões SERVER;

7.4.2.15.3 Timeout para conexões CLIENTS;

7.4.2.15.4 Timeout de conexão;

7.4.2.16 Deve possuir capacida de de inspeção de tráfego criptografado (SSL);

7.4.2.17 A inspeção do tráfego SSL deve ser inspecionado pelas mesmas políticas de filtragem aplicadas ao trafego não criptografado;

7.4.2.18 A Ferramenta deve possibilitar o uso de proxy streamino para os seguintes fins:

7.4.2.18.1 Redirecionamento de tráfego HTTP para HTTPS

7.4.2.18.2 Prevenção de acesso a ferramentas de Open Proxy

7.4.2.18.3 Balanceamento de carga

7.4.2.18.4 Caching

7.4.2.18.5 Criptografia SSL

7.4.2.18.6 Antimalware

7.4.2.19 A solução ofertada deve possuir filtro de reputação;

7.4.2.20 A solução ofertada deve possuir filtro de URL baseado em categorias, possuindo no minimo mais de 90 (noventa) categorias pré-definidas pelo fabricante;

7.4.2.21 As vacinas de malware e engine deverão ser desenvolvidos e fornecidos pelo fabricante da mesma solução, não sendo aceitas tecnologias OEM ou parceiros terceiros;

7.4.2.22 A solução deverá ter suporte mínimo as seguintes versões do SNMP:

7.4.2.22.1 SNMP v1;

7.4.2.22.2 SNMP v2c;

7.4.2.22.3 SNMP v3;

7.4.3 Características Gerais da Solução

7.4.3.1 Deverá suportar a interceptação e inspeção de no mínimo os protocolos:

7.4.3.1.1 HTTP;

7.4.3.1.2 HTTPS;

7.4.3.1.3 FTP;

7.4.3.2 Instant Messenger;

7.4.3.3 Deve suportar FTP over HTTP nos modos ativo/passivo.

7.4.3.4 Deve possibilidade a configuração das portas utilizadas para o serviço de Proxy.

7.4.3.5 Deve Possuir a capacidade de utilizar o proxy com o método CONNECT para portas especificas.

7.4.3.6 Permitir requisições dos clientes da rede interna em uma interface de rede e a comunicação com a Internet em outra interface, possibilitando usar um endereço IP privado na interface de rede interna e um IP público na interface de rede externa.

7.4.3.7 Deve ser capaz de criar lista de destinos que poderão exceder as regras de proxy e políticas baseadas no mínimo em:

7.4.3.7.1 Endereço IP;

7.4.3.7.2 CIDR (Classless Inter-Domain Routing);

7.4.3.7.3 Domínio;

7.4.3.7.4 Hostname completo ou parte;

7.4.3.8 Possuir a capacidade de atuar como proxy explícito e transparente.

7.4.3.9 Atuar como proxy transparente através do redirecionamento de conexões utilizando WCCP.

7.4.3.10 Deve possuir integração com serviços de diretório LDAP e domínios Windows 2008 para auditoria e autenticação sem a necessidade de instalação de agentes ou plugins em estação de trabalho ou servidor.

7.4.3.11 A solução deverá ser capaz de criar e hospedar arquivos PAC (Proxy Auto-configuration).

7.4.3.12 Deverá suportar IP Spoofing para implementação em modo transparente.

7.4.3.13 Deve possuir a capacidade de detecção automática de tráfego de streaming, com a finalidade de realizar bypass de Antimalware e controle de banda para esse tipo de tráfego.

7.4.4 Características da Filtragem e Reputação de URL

7.4.4.1 A base de URLs, deve ser atualizada automaticamente via Internet, por meio de uma base proprietária do fornecedor que suporte os serviços descritos neste termo e os equipamentos listados.

7.4.4.2 A base de URLs deve manter o conhecimento de pelo menos 90 (noventa) categorias pré-definidas e no mínimo 20 (vinte) milhões de domínios de URL's cadastradas;

7.4.4.3 Deve possibilitar a criação de no mínimo 500 (quinhentas) categorias extras customizadas (definidas pelo usuário)

7.4.4.4 A ferramenta deve ser capaz de realizar controle de banda para download/upload

7.4.4.5 O Controle de Banda deve ser granular, ou seja, podendo ser aplicado com restrições aos seguintes parametros:

7.4.4.5.1 Grupo de usuários;

7.4.4.5.2 Horário;

7.4.4.5.3 Categoria do Site;

7.4.4.6 Deve ser possível enviar para o fabricante da solução as URL´s não cadastradas na base de dados para análise e inclusão na base de categorias;

7.4.4.7 Deve permitir a criação de filtros URL's baseado em políticas de tempo, tais como dias da semana e range de horário, ou seja, alguns sites só poderão ser acessados fora do horário de expediente

7.4.4.8 Deverá ser capaz de criar ações diferentes para as URL´s em políticas por tempo.

7.4.4.9 Deve ser capaz de realizar a detecção de URLs frente a composição dos seguintes itens:

7.4.4.9.1 Url

7.4.4.9.2 Host

7.4.4.9.3 Domínio

7.4.4.9.4 Protocolo

7.4.4.9.5 Caminho da URL

7.4.4.10 Deverá possuir modelo de resposta padrão aos usuários;

7.4.4.11 Deverá permitir customização das páginas de notificações existentes e a criação de novas páginas de resposta;

7.4.4.12 A solução deverá detectar, monitorar e interceptar o acesso feito às páginas abertas dentro de servidores remotos, como:

7.4.4.12.1 Servidores de tradução;

7.4.4.12.2 Proxies anônimos;

7.4.4.13 As transações que forem detectadas deverão estar de acordo com as políticas estabelecidas pela empresa, onde o conteúdo não permitido que for acessado sob este mecanismo deverá ser bloqueado e o conteúdo dentro de políticas que permitem o acesso deverão ser acessados.

7.4.4.14 Deve possuir, no mínimo, as seguintes categorias URL:

7.4.4.14.1 Sites de conteúdos maliciosos;

7.4.4.14.2 Site de bate-papo (chat) e fóruns on-line;

7.4.4.14.3 Sites de Anonymizers;

7.4.4.14.4 Sites com utilitários para Anonymizing;

7.4.4.14.5 Browser Exploits;

7.4.4.14.6 Sites de Encontros (Dating);

7.4.4.14.7 Sites de Discriminação;

7.4.4.14.8 Sites sobre Drogas 9;

7.4.4.14.9 Sites sobre Apostas 10;

7.4.4.14.10 Sites sobre conteúdo agressivo (Gruesome Content);

7.4.4.14.11 Site com downloads maliciosos;

7.4.4.14.12 Site com download de media;

7.4.4.14.13 Sites de compartilhamento de medias;

7.4.4.14.14 Instant Messaging;

7.4.4.14.15 P2P/File Sharing;

7.4.4.14.16 Sites para armazenamento de dados pessoais (Personal Network Storage);

7.4.4.14.17 Sites sobre Potenciais Atividades Criminais;

7.4.4.14.18 Sites sobre Potenciais Crimes de Hacking/Computer Crime;

7.4.4.14.19 Sites sobre Potenciais Softwares Ilegais;

7.4.4.14.20 PUPS;

7.4.4.14.21 Endereços de IP Residencial;

7.4.4.14.22 Shareware/Freeware;

7.4.4.14.23 Spyware/Adware/Keyloggers;

7.4.4.14.24 Web Mail

7.4.4.15 Deve possuir um sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino, utilizando dados de uma rede mundial de monitoração de tráfego web e de e-mail para definir a reputação dos servidores de destino com cobertura global.

7.4.4.16 Permitir ações diferenciadas de acordo com cada reputação obtida, como bloquear, permitir ou verificar detalhadamente os objetos de cada acesso

7.4.4.17 O produto deve ser capaz de realizar controle de aplicações web, aplicando políticas por:

7.4.4.17.1 Aplicações;

7.4.4.17.2 Usuários;

7.4.4.17.3 Grupos de risco de aplicação;

7.4.4.18 O Filtro de aplicação deve permitir configurar permissão de acesso de somente leitura para aplicações específicas.

7.4.4.19 Deve possuir capacidade de classificação de conteúdo dinâmico, aplicando auto-categorização aos websites que eventualmente estejam fora da lista local/nuvem.

7.4.4.20 Deve possuir serviço de inteligência do fabricante da solução, nativo ao produto, para informação de URL's de alto risco e médio risco;

7.4.4.21 Ao detectar uma URL de alto risco ou médio risco o mesmo deve solicitar ao usuário que ele aceite os termos da política de acesso e entenda os riscos antes de acessar tais websites;

7.4.4.22 Deve ser capaz de efetuar bloqueios e controle de Web 2.0, como por exemplo:

7.4.4.22.1 Liberar apenas canais específicos do Youtube;

7.4.4.22.2 Bloqueio de determinados canais do Youtube;

7.4.4.22.3 Bloqueio de vídeos do YouTube por palavras chave;

7.4.4.22.4 Bloqueio do Chat do facebook;

7.4.4.22.5 Bloqueio da Criação de Eventos do facebook;

7.4.5 Características de Autenticação e Integração

7.4.5.1 A solução deverá possuir todos os métodos abaixo citados:

7.4.5.1.1 Autenticação do usuário via NTLM de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha para o usuário;

7.4.5.1.2 Autenticação segura de clientes, ou seja, os dados de autenticação trocados entre o servidor de diretórios e o proxy criptografados, tanto para LDAP como para NTLM;

7.4.5.1.3 Autenticação baseada em LDAP;

7.4.5.1.4 Utilização de um NTLM-Agent, sendo um agente externo instalado em um sistema baseado em Windows para aplicação do método de autenticação NTLM;

7.4.5.1.5 Banco de dados de usuários em uma base na própria solução;

7.4.5.1.6 Através de servidores LDAP;

7.4.5.1.7 Através de servidores Novell eDirectory;

7.4.5.1.8 Através de servidores RADIUS;

7.4.5.1.9 Através de servidores Kerberos;

7.4.5.1.10 Através de servidores de Autenticação Externo;

7.4.5.1.11 Através do uso de cookies;

7.4.5.2 A autenticação deve possuir compatibilidade com todos os métodos abaixo descritos:

7.4.5.2.1 Básica (Basic Authentication) utilizando tecnica de POPUP

7.4.5.2.2 NTLM over Proxy

7.4.5.2.3 Kerberos over HTTP

7.4.5.3 Autenticação (login, senha e domínio) para usuários que estejam utilizando sistemas operacionais diferentes do Windows (Linux, por exemplo), validando estes usuários no serviço de diretórios Microsoft Active Directory 2000/2003/2008.

7.4.5.4 Autenticação de usuários e estações de trabalho sem a necessidade de instalação e/ou execução de clientes ou quaisquer módulos em nenhuma estação de trabalho e/ou servidor.

7.4.5.5 Total integração com o Microsoft Active Directory 2008 para autenticação de usuários e grupos, sem a necessidade de instalação e/ou execução de clientes ou quaisquer módulos nas estações de trabalho dos usuários ou nos servidores

7.4.6 Características da Criação de Regras e Listas

7.4.6.1 A solução ofertada deve possuir mecanismo de criação de regras a partir de logica booleana permitindo flexibilidade e otimizacao a partir de parâmetros pre definidos;

7.4.6.2 A solução deve permitir a criação dos conjuntos de regras e regras de forma ordem dependente;

7.4.6.3 A solução deve permitir a criação de conjunto de regras baseados em critérios para habilitação da mesma;

7.4.6.4 Estes critérios devem ser aplicados para Requisições, Respostas e Objetos incorporados de todas operações realizadas pelo produto ofertado;

7.4.6.5 O produto deve possuir pelo menos 400 propriedades para serem utilizadas pelas regras ou para os critérios de utilização das mesmas;

7.4.6.6 Aplicação do conjunto de regras deve se basear em todas as propriedades e permitir a criação de lógica booleana entre estas propriedades e seus valores para decisão de habilitação ou não deste conjunto de regras;

7.4.6.7 Cada propriedade deverá ser testada através de operadores (igual, diferente, pertence a lista, não pertence a lista, maior que, maior que ou igual, menor que, ou menor que ou igual) para ser considerada válida ou não e com isso tomar a decisão se este conjunto de regras será testado ou não.

7.4.6.8 O produto deve possuir pelo menos as seguintes classes de propriedades abaixo citadas:

7.4.6.8.1 Antimalware

7.4.6.8.2 Probability

7.4.6.8.3 Authentication

7.4.6.8.4 BytestoClient

7.4.6.8.5 Block

7.4.6.8.6 Body

7.4.6.8.7 Cache

7.4.6.8.8 Category

7.4.6.8.9 Command

7.4.6.8.10 Client

7.4.6.8.11 Cache

7.4.6.8.12 DateTime

7.4.6.8.13 Error

7.4.6.8.14 HTML

7.4.6.8.15 Header

7.4.6.8.16 ICAP

7.4.6.8.17 IM

7.4.6.8.18 List

7.4.6.8.19 MediaType

7.4.6.8.20 PDStorage

7.4.6.8.21 ProgressPage

7.4.6.8.22 Proxy

7.4.6.8.23 Quota

7.4.6.8.24 Rules

7.4.6.8.25 Request

7.4.6.8.26 Response

7.4.6.8.27 SNMP

7.4.6.8.28 String

7.4.6.8.29 URL

7.4.6.9 A combinação de testes de propriedades deve permitir a validação das mesmas através de lógica definida pelo administrador da solução através de uso de operadores OR ou AND e permitir

a combinação dos mesmos como exemplos abaixo: 1. a OR b OR c 2. (a OR b) AND c 3. (a AND b) OR c

7.4.6.10 Após validação desta regra o produto deve tomar as seguintes ações:

7.4.6.10.1 Autenticar;

7.4.6.10.2 Bloquear;

7.4.6.10.3 Continuar;

7.4.6.10.4 Redirecionar;

7.4.6.10.5 Remover;

7.4.6.10.6 Parar analise do ciclo;

7.4.6.10.7 Parar análise do conjunto de regras;

7.4.6.11 A solução deve permitir o uso de listas nas regras utilizando a mesma lógica booleana acima explicadas:

7.4.6.11.1 Categorias

7.4.6.11.2 Autoridades Certificadoras

7.4.6.11.3 Hosts e certificados confiaveis

7.4.6.11.4 Endereços Ips

7.4.6.11.5 Ranges Ips

7.4.6.11.6 Usuarios locais

7.4.6.11.7 Tipo de midia

7.4.6.11.8 Numeros

7.4.6.11.9 Strings

7.4.6.11.10 Expressões Regulares (utilizando REGEX e/ou GLOB)

7.4.6.12 A solução deve possuir mecanismo de DLP nativo sem necessidade de licença adicional

7.4.6.13 A solução deve ser capaz de integrar-se a ferramenta de DLP de Rede respondendo ao modo Request e Response

7.4.6.14 A ferramenta deve ser capaz bloquear o envio de documentos para Web baseado em extensão ou tipo de documento.

7.4.6.15 A solução deve ser capaz de criptografar arquivos enviados a sites de armazenamento, como por exemplo:

7.4.6.15.1 Dropbox;

7.4.6.15.2 Microsoft One Drive;

7.4.6.15.3 Box;

7.4.6.15.4 Google Drive;

7.4.6.16 Ao criptografar um arquivo o mesmo só poderá ser de-criptografado após passagem pela solução de Filtragem Web;

7.4.6.16.1 Este módulo deverá ser nativo da solução e não requerer nenhum equipamento externo;

7.4.6.17 Deve ser capaz de bloquear páginas por meio de Geolocalização;

7.4.7 Características do módulo Anti-Malware

7.4.7.1 A solução deverá possuir um módulo de análise de malwares desenvolvido pelo fabricante da solução, não sendo aceitos OEM's;

7.4.7.2 A solução deve oferecer a opção de no mínimo dois mecanismos de anti-vírus rodando simultaneamente possibilitando uma camada adicional de filtragem;

7.4.7.3 Se houver algum atraso ou falha na realização da atualização automática, o equipamento deve ter a capacidade de alertar imediatamente o administrador através de logs, SNMP e E-mail.

7.4.7.4 Deve realizar a análise de comportamento (emulação) das páginas que serão acessadas;

7.4.7.4.1 Identificar e bloquear aplicações Java Scripts maliciosas;

7.4.7.4.2 Identificar e bloquear aplicações Java applets maliciosas;

7.4.7.4.3 Identificar e bloquear aplicações Java applications maliciosas;

7.4.7.4.4 Identificar e bloquear aplicações ActiveX maliciosas;

7.4.7.4.5 Identificar e bloquear aplicações Flash ActionScripts

7.4.7.4.6 Identificar e bloquear aplicações executáveis Windows maliciosas;

7.4.7.4.7 Identificar e bloquear scripts Visual Basic maliciosos;

7.4.7.4.8 Identificar e bloquear aplicações Potencialmente Não Desejados (spywares, etc...);

7.4.7.5 Deve possuir tecnologia de análise em nuvem para arquivos suspeitos. Esta tecnologia deve se basear no envio do hash do arquivo/código para o o serviço de inteligência do fabricante a fim do mesmo validar se o arquivo é malicioso ou não e prover o bloqueio/controle sem a necessidade de vacina instalada na solução ofertada.

7.4.7.6 Possuir filtros de analise de intenções para proteção pró-ativa contra ataques de dia zero com bloqueio de tráfego web em tempo real sem a necessidade de possuir uma assinatura;

7.4.7.7 A varredura deverá ser feita seqüencialmente no sistema, sem o uso de protocolos de comunicação entre as ferramentas como ICAP.

7.4.7.8 Detectar e bloquear "user agent" suspeitos/não autorizados.

7.4.7.9 A solução deve possibilitar bloquear todos os comportamentos/técnicas abaixo descritas:

7.4.7.9.1 Data theft: Backdoor

7.4.7.9.2 Data theft: Keylogger

7.4.7.9.3 Data theft: Password stealer

7.4.7.9.4 System compromise: Code execution exploit

7.4.7.9.5 System compromise: Browser exploit

7.4.7.9.6 System compromise: Trojan

7.4.7.9.7 Stealth activity: Rootkit

7.4.7.9.8 Viral Replication: Network worm

7.4.7.9.9 Viral Replication: File infector virus

7.4.7.9.10 System compromise: Trojan downloader

7.4.7.9.11 System compromise: Trojan dropper

7.4.7.9.12 System compromise: Trojan proxy

7.4.7.9.13 Web threats: Infected website

7.4.7.9.14 Stealth activity: Code injection

7.4.7.9.15 Detection evasion: Obfuscated code

7.4.7.9.16 Detection evasion: Packed code

7.4.7.9.17 Potentially unwanted: Ad-/Spyware

7.4.7.9.18 Potentially unwanted: Adware

7.4.7.9.19 Data theft: Spyware

7.4.7.9.20 Potentially unwanted: Dialer

7.4.7.9.21 Web threats: Vulnerable ActiveX controls

7.4.7.9.22 Potentially unwanted: Suspicious activity

7.4.7.9.23 Web threats: Cross-site scripting

7.4.7.9.24 Potentially unwanted: Deceptive behavior

7.4.7.9.25 Potentially unwanted: Redirector

7.4.7.9.26 Potentially unwanted: Direct kernel communication

7.4.7.9.27 Potentially unwanted: Privacy violation

7.4.8 Características da Gerência da Solução

7.4.8.1 Possuir interface de gerência via Web e linha de comando.

7.4.8.2 Possuir MIB própria para verificação das informações de utilização via SNMP.

7.4.8.3 Possibilitar o envio de alertas administrativos utilizando e-mails e traps SNMP.

7.4.8.4 Possibilitar a criação de políticas de acesso a interface de gerenciamento baseada em endereço IP e range de IP's que podem acessar o sistema.

7.4.8.5 O Fabricante deve permitir a consulta da categoria de um determinado site através de servidor público próprio na internet;

7.4.8.6 Deverá possuir pelo menos sete perfis de usuários de acesso;

7.4.8.7 A solução deverá permitir autenticação externa, para autenticar os usuários ao logar na gerência da solução através dos seguintes métodos de autenticação:

7.4.8.7.1 Através de servidores NTLM;

7.4.8.7.2 Banco de dados de usuários em uma base na própria solução;

7.4.8.7.3 Através de servidores LDAP;

7.4.8.7.4 Através de servidores Novell eDirectory ;

7.4.8.7.5 Através de servidores RADIUS;

7.4.8.7.6 Através de servidores Kerberos;

7.4.8.8 Deve prover as seguintes informações:

7.4.8.8.1 Quantidade de Requisições/Segundo

7.4.8.8.2 Alertas;

7.4.8.8.3 Erros;

7.4.8.8.4 Informações sobre a Engine de Analise de Malware

7.4.8.8.5 Versão do Filtro URL

7.4.8.9 Relatórios pré-configurados com as seguintes informações:

7.4.8.9.1 Sumário Executivo de Acessos

7.4.8.9.1.1 Sumário de Acessos a URL's

7.4.8.9.1.2 Sumário das Categorias Acessadas

7.4.8.9.1.3 Sumário dos Malwares Acessados;

7.4.8.9.2 Sumário do Sistema

7.4.8.9.2.1 Utilização de Rede (Volume de Tráfego)

7.4.8.9.2.2 Utilização do Sistema

7.4.8.9.2.3 Status do Update

7.4.8.9.3 Sumário Web

7.4.8.9.3.1 Tráfego por protocolo

7.4.8.9.3.2 Requests por protocolo

7.4.8.9.4 Volume de Tráfego

7.4.8.9.4.1 Bytes transferidos por domínio

7.4.8.9.4.2 Bytes transferidos por IP de origem

7.4.8.9.4.3 Bytes transferidos por IP de destino

7.4.8.9.5 Estatísticas de uso de CACHE

7.4.8.9.6 Estatísticas do Filtro URL

7.4.8.10 Deve possuir capacidade de realizar a captura de sessão de usuário e identificar possiveis problemas na aplicação de uma regra em específico;

7.4.8.11 Deve suportar captura de pacotes para mitigação de problemas de conexão (tcpdump);

7.4.8.12 Deve permitir a realização de backup e restauração da configuração a partir da própria console de gerência;

7.4.8.13 Deve possuir log de auditoria de todas as ações realizadas na console com, no mínimo, as seguintes informações:

7.4.8.13.1 Data e Hora;

7.4.8.13.2 Usuário;

7.4.8.13.3 Ação;

7.4.8.13.4 IP Origem;

7.4.8.13.5 Detalhes da ação;

7.4.8.14 Deve permitir a configuração de Network Bonding através da console;

7.4.8.15 Deve suportar a configuração de Source-based routing pela console;

7.4.8.16 Deve permitir a configuração da quantidade de threads a ser utilizada para a análise de malware;

7.4.8.17 Deve permitir informar ao usuário a tela de progresso da análise de um arquivo;

7.4.8.18 Deve ser possível configurar o tempo máximo de retenção de logs e a sua auto deleção após um período pré-definido de tamanho;

7.4.9 Característica do Módulo de Relatórios

7.4.9.1 A solução apresentada deverá possuir um mecanismo para geração de relatórios e logs

7.4.9.2 Serão aceitos módulos de relatórios que rodem fora do apliance (out-of-box), desde que seja do mesmo fabricante

7.4.9.3 Deve possuir ferramenta para análise de tráfego interativo, visando identificar o resultado das regras aplicadas, facilitando a metodologia de análise de problemas.

7.4.9.4 O módulo de relatório deverá se adequar aos padrões do SINE-IDT/CE, com suporte completo de instalação a todos os seguintes sistemas operacionais e Bases de dados:

7.4.9.4.1 Windows 2008 Server

7.4.9.4.2 Windows 2012 Server

7.4.9.4.3 Microsoft SQL Server 2008

7.4.9.5 Deverá permitir a criação dos relatórios nos formatos:

7.4.9.5.1 HTML

7.4.9.5.2 PDF

7.4.9.5.3 CSV;

7.4.9.6 Deverá possuir no mínimo 30 relatórios pré-definidos, permitindo ao administrador configurar novos relatórios;

7.4.9.7 Permitir filtrar todos os relatórios com base em:

7.4.9.7.1 Sites

7.4.9.7.2 Nomes de usuários

7.4.9.7.3 Endereços Ips

7.4.9.7.4 Protocolo de Aplicação

7.4.9.7.5 Tipo de arquivos

7.4.9.7.6 Categorias

7.4.9.7.7 Malware

7.4.9.7.8 Reputação Web

7.4.9.7.9 Fonte de logs enviados (por appliance utilizado como fonte destes dados)

7.4.9.8 Permitir de forma opcional a criação de contas na ferramenta de relatório (reporting account) com restrição ao acesso a partes especifica dos dados com todos os filtros abaixo:

7.4.9.8.1 Usuários individuais ou grupos de usuários (usuários internos da ferramenta ou sincronizados com os de serviço de diretório como LDAP, AD, etc...)

7.4.9.9 Permitir atribuir colunas predefinidas, excluir colunas ou renomear colunas dos arquivos de log nos arquivos existentes. Isso deverá ser feito a partir de um assistente de customização de logs.

7.4.9.10 Deverá prover uma interface de monitoramento (Dashboard), monitorando a atividade de acesso web, incluindo:

7.4.9.10.1 Categorias;

7.4.9.10.2 Sites maliciosos – tentativas de acesso;

7.4.9.10.3 Sites acessados.

7.5 Serviço de Monitoria e Análise Pro Ativa dos Eventos de Segurança

7.5.1 Características Gerais

7.5.1.1 Todo o gerenciamento dos componentes e funções administrativas devem ser feitas através de uma única interface web, acessível por navegador, sem a necessidade de instalação de aplicação adicionais;

7.5.1.2 A solução deverá ser fornecida para instalação e uso no idioma Português Brasil (pt_br) e Inglês;

7.5.1.3 A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante;

7.5.1.4 Controlar o acesso dos usuários da solução por meio da integração com bases: Microsoft Active Directory, LDAP, TACACS, RADIUS e base de dados local;

7.5.1.5 A solução deve sincronizar o horário de seus componentes utilizando o serviço NTP ou RDate da organização;

7.5.1.6 A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web única, sem necessidades de intervenção nos equipamentos onde está instalado;

7.5.1.7 Os componentes de Console, Coletor, Correlacionador e armazenamento de logs e flows de rede devem ser fornecidos em Alta-disponibilidade, ou seja, mesmo com a falha de um dos componentes da solução, toda a solução deve continuar funcionando de forma automática, sem a necessidade de intervenção manual;

7.5.1.8 Os componentes da solução poderão ser executados num mesmo equipamento, ou podem ser distribuídos em múltiplos equipamentos, de acordo com a característica de cada produto, respeitadas as características de funcionamento e performance exigidas;

7.5.1.9 Ao utilizar de mais de um componente na solução, a comunicação deverá ser feita de forma criptografada, garantindo a autenticidade, confidencialidade e integridade dos dados;

7.5.1.10 Para o acesso à interface web de administração, deve permitir o uso de certificado digital emitido por autoridade certificado interna do SINE-IDT/CE ou por autoridade certificadora reconhecida pelos navegadores;

7.5.1.11 Deve permitir sua monitoração por SNMPv2c e SNMPv3;

7.5.1.12 A arquitetura da solução deverá suportar uma implementação "Multi-Tenancy". Sendo assim será possível customizar fontes de evento, fontes de flows rede, regras de correlação específicas para diferentes clientes ou áreas de negócio, as quais estarão utilizando um ambiente compartilhado.

7.5.1.13 Deve permitir a configuração de volumetria por "tenancy" criado, isto é, possibilitando que seja configurado o volume de eventos e flows de rede serão processados por clientes gerenciados ou áreas específicas da empresa.

7.5.1.14 A solução deve ser licenciada com a capacidade de coletar, processar e correlacionar 100 eventos por segundo.

7.5.1.15 A solução deve prover aceleradores de implementação, boas práticas e aumento da inteligência, através de integrações adicionais, dashboards e aplicações de terceiros extras, em

formato de plug-in ou "App". Esses plug-ins devem estar disponíveis em um site público na Internet, e a instalação deve ser realizada através da interface gráfica da solução.

7.5.2 Correlação de eventos

7.5.2.1 A coleta, normalização e o correlacionamento dos eventos provenientes dos dispositivos monitorados devem ser realizadas próximos ao tempo real;

7.5.2.2 Os eventos devem ser normalizados e categorizados em um padrão único que será usado pela solução;

7.5.2.3 Permitir a agregação de eventos semelhantes;

7.5.2.4 Deve possuir no mínimo 64 GB de memória RAM;

7.5.2.5 Deve atribuir métrica de prioridade para os eventos e para os alertas/incidentes;

7.5.2.6 Gerar alertas/incidentes com base nas regras definidas previamente;

7.5.2.7 Verificar conformidade com as políticas, controles e normas internas (customizadas) e regulamentações externas (ex. ISO 27001, PCI, SOX, HIPAA);

7.5.2.8 Deverá ser fornecido com módulo integrado para o gerenciamento dos incidentes identificados pela solução.

7.5.2.9 Deve permitir armazenar os eventos, inclusive os normalizados, de forma compactada;

7.5.2.10 Apresentar painéis gráficos (dashboards) com indicativos de situações relacionados à segurança, compliance, aplicações e monitoração do próprio sistema;

7.5.2.11 Os painéis gráficos (dashboards) devem ser customizáveis, por usuário;

7.5.2.12 Permitir a análise de eventos baseados em contexto, tais como, usuários, localização geográfica, bem como qualquer outro metadado contido no evento;

7.5.2.13 Permitir a visualização, na interface web, dos eventos relacionados a um alerta e/ou incidente de segurança, identificado pelas regras de correlação da solução;

7.5.2.14 Enviar notificações relacionadas a um incidente/alerta por e-mail, trap snmp e syslog;

7.5.2.15 A solução deverá ter, no mínimo, as seguintes formas de coleta de eventos: Syslog (UDP, TCP), Syslog criptografado com TLS, JDBC, SNMP (v1, v2 e v3), Microsoft Event Log, Arquivos de Log em formato de texto, Checkpoint OPSEC/LEA, CISCO NSEL e Juniper NSM Protocol;

7.5.2.16 Ter a capacidade de reenviar os eventos, em formato "raw", para outros sistemas de correlacionamento;

7.5.2.17 Ter a capacidade de reenviar eventos já normalizados para outros sistemas de correlacionamento;

7.5.2.18 Deve permitir a configuração de ofuscação de qualquer parte dos dados recebidos, assim que normalizados.

7.5.2.19 A ofuscação de dados deve ser configurada com chaves de criptografia;

7.5.2.20 Possuir a capacidade de automatizar a resposta a incidentes, através da execução de scripts, como ação customizada dentro das regras de correlação.

7.5.2.21 Possuir a capacidade de customizar e personalizar diferentes "templates" de email que será enviado como resposta aos incidentes identificado.

7.5.3 Coleta de logs

7.5.3.1 Componente da solução que tem como função básica fazer a interface com o dispositivo monitorado, recebendo ou buscando eventos relevantes que serão inseridos na solução, contendo obrigatoriamente documentação de todos coletores nativos com informações de configurações de cada ativo suportado e como deve ser feita no mesmo.

7.5.3.2 Filtrar e selecionar os eventos que serão inseridos na solução ou que serão retidos na base de dados da solução por períodos previamente definidos. Deve permitir a criação e alteração de políticas de retenção;

7.5.3.3 Normalizar e categorizar os eventos em um padrão único que será usado pela solução;

7.5.3.4 Possuir suporte nativo para reconhecimento e coleta de, pelo menos, 250 tipos de fontes de dados diferentes;

7.5.3.5 Tratar eventos em formato "comprimido" (zip, gz, tar.gz), sem a necessidade da descompressão manual;

7.5.3.6 Deverá fazer a agregação de eventos, mostrando a contagem de eventos, quando o mesmo evento ocorrer dentro de um período curto. A opção de realizar ou não a agregação de eventos deve ser configurável, por dispositivo integrado;

7.5.3.7 Deve ser capaz de manter o evento bruto ("raw") para o armazenamento e consulta futura;

7.5.3.8 Deve ser capaz de agregar informações sobre localização geográfica dos endereços IP envolvidos no evento, para que a mesma seja usada no correlacionamento;

7.5.3.9 Um único componente da solução deve ser capaz de coletar, processar e normalizar tanto os eventos de segurança e eventos de negócio (não relacionados à segurança);

7.5.3.10 Tanto os eventos de segurança quanto os de negócios devem ser normalizados para um único padrão de eventos.

7.5.3.11 A solução deve permitir a integração de dispositivos ou logs não suportados nativamente;

7.5.3.12 Essa integração deve ser realizada na interface web ou pelo uso de arquivos de configuração, com o uso de expressões regulares (ou recurso similar), sem exigir o uso de linguagens de programação ou scripts, tais como Java, C, PowerShell, shell scripts, etc.

7.5.3.13 A mesma integração deve suportar as seguintes formas de coleta de eventos: Syslog (UDP, TCP), Syslog criptografado com TLS, JDBC, SNMP (v1, v2 e v3), Microsoft Event Log, Arquivos de Log em Formato de texto, Check Point OPSEC/LEA, CISCO NSEL, Juniper NSM Protocol;

7.5.3.14 A solução deve suportar, nativamente, pelo menos as seguintes fontes de logs: Windows, Linux, IBM/AIX, IBM/RACF, HPUX, Solaris, Oracle Database, IBM/DB2, MS SQL Server, Firewalls (Checkpoint, Cisco/ASA, Juniper, Fortinet e Palo Alto e SonicWall), Network IPS (Sourcefire, IBM/ISS, HP Tipping Point, Snort e McAfee);

7.5.3.15 A solução deve suportar "overlap de IP", isto é, rotular os eventos para que seja possível gerenciar eventos de fontes de log que estejam em redes diferentes, mas possuem o mesmo endereçamento IP.

7.5.4 Coleta e análise de Fluxos de Rede:

7.5.4.1 Componente para coleta e análise de fluxos de rede, integrado à solução ofertada;

7.5.4.2 Deve exibir perfil do tráfego em tempo real, e normalizada de forma agregada. Deve incluir informações de bytes, pacotes e protocolos;

7.5.4.3 Suportar a identificação de aplicativos pelo uso de portas do tipo "well-known", e independentemente da porta, pela inspeção do tráfego. Aplicativos tunelados ou escondidos em outras portas, exemplo HTTP como transporte para o Instant Messenger, deve ser detectado adequadamente, nesse caso como Instant Messenger;

7.5.4.4 Deve ser capaz de reconhecer o protocolo da aplicação (camada 7) através da análise do protocolo/conteúdo, sem a necessidade de indicação da porta tcp/ip, para no mínimo 800 aplicações;

7.5.4.5 Suportar a definição de novos aplicativos/protocolos, pela especificação da porta e pela especificação de características do protocolo;

7.5.4.6 Deve permitir o armazenamento do conteúdo capturado na análise de flows camada 7, no formato nativo "raw";

7.5.4.7 Deve ser capaz de reconhecer aplicações encapsuladas em protocolo web, como por exemplo, MSN Live, Google, Facebook e Instant Messages;

7.5.4.8 Aprender de forma dinâmica regras de comportamento e expor alterações quando estas ocorrerem;

7.5.4.9 Junto com a solução de correlação de eventos, deve auxiliar a detecção de ataques de negação de serviço (DoS) e de negação de serviço distribuído (DDoS);

7.5.4.10 Detectar e apresentar visões de tráfego relativas a ameaças observadas na rede;

7.5.4.11 Deve suportar o recebimento dos seguintes padrões de flow: Netflow (versão 5 e 9), IPFIX, J-Flow, sFlow (versões 2, 4 e 5) e Packeteer;

7.5.4.12 Monitorar a rede e identificar padrão de tráfego que possa ser uma ameaça, bem como detectar tráfego de rede de aplicativos como compartilhamento de arquivos, P2P e jogos;

7.5.4.13 Deve ser capaz de apresentar informações de fluxo de rede por período de tempo pré-definido;

7.5.4.14 Deve ser capaz de montar visualizações de fluxo de rede baseados em comunicações provenientes ou destinadas à internet agrupado por regiões geográficas;

7.5.4.15 Deve possuir a capacidade de extrair dados, definidos pelo usuário, a partir dos dados da camada de aplicação recebidos por flow e associar estes a campos/metadados, que poderão ser usados em regras de correlação;

7.5.4.16 Possuir appliance especializado na geração de flows de rede a partir da captura de tráfego, produzindo informações da camada de aplicação (camada 7 do modelo OSI), suportando, no mínimo, a inspeção de 10Gbps de tráfego capturado;

7.5.4.17 O appliance especializado na geração de flows deve possuir no mínimo 2 interfaces de rede 10Gbps de fibra, para captura de tráfego;

7.5.5 <u>Correlacionamento</u>:

7.5.5.1 Componente responsável pelo correlacionamento dos eventos coletados, criando incidentes de segurança a partir da análise automática dos dados da solução.

7.5.5.2 Deve correlacionar eventos provenientes das fontes de logs e flows, gerando incidentes;

7.5.5.3 Efetuar o correlacionamento dos eventos próximo ao tempo real;

7.5.5.4 Deve possuir, pelo menos, 500 (quinhentas) regras de correlação pré-definidas nativamente;

7.5.5.5 Deve permitir a criação de novas regras e a edição das existentes;

7.5.5.6 Deve permitir o correlacionamento de qualquer informação que conste no evento, inclusive informações que não sejam referentes a endereçamento IP, portas, etc, tais como dados financeiros;

7.5.5.7 Deve permitir a criação de regras que identifiquem mudanças de comportamento, como surto ou ausência de eventos/tráfego, quando comparados a outros períodos similares (ex. mesmo período do dia, mesmo dia da semana);

7.5.5.8 Deve permitir a criação de regras que identifiquem desvios, em qualquer metadado, de limites pré-estabelecidos;

7.5.5.9 Deve ter a capacidade de detectar automaticamente padrões de ataques especializados que acontecem ao longo do tempo e não foram previstos ou observados anteriormente;

7.5.5.10 Integrar com ferramentas externas como Nslookup, Whois, Nmap;

7.5.5.11 Permitir o correlacionamento de eventos e alertas com dados existentes em listas (watchlist), permitindo também a criação de novas listas e a edição das existentes, de forma automatizada e manual;

7.5.5.12 Capacidade de fazer o correlacionamento entre eventos e fluxos de rede, como: NetFlow, J-Flow, S-Flow e IPFIX, sem a necessidade de ferramentas de terceiros ou qualquer componente adicional ao licenciamento da solução;

7.5.5.13 Correlacionar eventos oriundos de mais de uma fonte, tipo ou localização;

7.5.5.14 Priorizar os eventos e incidentes com base, pelo menos, nos seguintes critérios: severidade e criticidade/relevância do evento ou incidente. Podendo ser utilizada uma combinação desses critérios;

7.5.5.15 Os incidentes devem ser agrupados, no mínimo, por: categoria, endereço de origem, endereço de destino;

7.5.5.16 Possuir pelo menos os seguintes tipos de correlação:

7.5.5.16.1 Correlação por regras;

7.5.5.16.2 Extrapolação de um limite (threashold);

7.5.5.16.3 Correlação por anomalia e padrão de comportamento;

7.5.5.17 Como resultado das regras, deve ser capaz de executar ações automáticas, no mínimo: enviar e-mail, enviar mensagem para o usuário conectado no console, criar um incidente no sistema de workflow interno, enviar traps SNMP e popular listas (watch list);

7.5.5.18 Integrar-se com pelo menos um ou mais sistemas de inteligência com informações de riscos globais tais como: HP ThreatLink (DVLabs), Symantec DeepSight, Verisign iDefense, IBM X-Force;

7.5.5.19 Qualquer metadado dos eventos deve poder ser usado em uma regra de correlação.

7.5.5.20 Deve permitir testar as regras de correlação em eventos passados, em período de tempo e escopo bem definidos.

7.5.5.21 Deve permitir usar as regras de correlação com eventos reais capturados anteriormente e mantidos na base de dados da solução, sem afetar a execução das regras em produção e o fluxo de dados online. Deve permitir especificar qual horário a ser utilizado para a correlação, o da recepção do evento na solução ou o horário original do evento.

7.5.6 **Armazenamento de dados**:

7.5.6.1 Arquitetura e forma de armazenamento de dados e informações dentro da solução

7.5.6.2 Armazenar os dados: eventos, flows, incidentes, workflow nativo e toda informação pertinente à solução, tais como configuração, usuários, trilhas de auditoria;

7.5.6.3 Devem ser armazenados os eventos e flows de acordo com política de retenção, com compressão, e excluídos após um período de tempo definido;

7.5.6.4 Deve ter capacidade de armazenar os eventos em formato original (“raw”);

7.5.6.5 Armazenar logs por tempo determinado e customizado;

7.5.6.6 Deve permitir o uso de algoritmo para garantia de integridade dos eventos armazenados, utilizando no mínimo os algoritmos: SHA-256, SHA-384 e SHA-512;

7.5.6.7 Deve permitir o uso dos algoritmos para garantia de integridade do item 1.2.71 com código de autenticação da mensagem (HMAC).

7.5.6.8 Deve possuir funcionalidade para expandir a capacidade de armazenamento de dados da solução, através da inserção de novos discos, appliance ou solução de armazenamento externo, sem necessidade de reconstruir a base de dados;

7.5.6.9 Deve permitir o expurgo de eventos (metadados e raw) de forma automática, permitindo a customização do período de expurgo por diversos fatores, no mínimo: tipo/nome do evento e dispositivo/fonte de log;

7.5.6.10 Deve registrar todas as interações dos usuários e administradores com a solução em trilhas de auditoria.

7.5.6.11 Além do armazenamento interno, deve possibilitar o uso de armazenamento externo, através de placa HBA ou iSCSI;

7.5.6.12 Deve possuir funcionalidade de backup integrada, que faça a cópia de segurança de: eventos, flows, incidentes e demais dados, além das configurações;

7.5.6.13 Deve permitir o armazenamento das cópias de segurança em armazenamento externo, conectado por interface HBA, iSCSI ou NFS.

7.5.6.14 Deve ter a capacidade de armazenar todo os dados coletados de forma online por até 30 dias, isto é, podendo esses dados serem utilizados de forma imediata para buscas, relatórios e correlação de eventos e flows rede.

7.5.6.15 Possuir mecanismos automatizados para backup dos dados em mídias off-line. Os dados serão mantidos por até 6 meses de forma off-line.

7.5.6.16 A solução deverá permitir a recuperação dos dados armazenados de forma off-line, e reinserção como dados online, isto é, quando necessário ser possível recuperar os dados armazenados em mídias off-line, e através de processos documentados reinseri-los na base de dados online para buscas, relatórios e investigações forenses.

7.5.7 Console de administração, gerenciamento e Operação:

7.5.7.1 Interface web única para administração, gerenciamento e operação da solução

7.5.7.2 Possuir acesso controlado e autenticado por usuário;

7.5.7.3 Possuir capacidade de integração com bases Microsoft Active Directory, LDAP, TACACS e RADIUS para autenticação de usuários;

7.5.7.4 Possuir acesso seguro e criptografado à interface web, de forma a garantir a confidencialidade;

7.5.7.5 Garantir acesso aos dados e às funcionalidades/ações diferenciadas por perfis de acesso;

7.5.7.6 O controle de acesso deve ser configurado na interface web, com capacidade para limitar os recursos da solução a perfis de usuários, conforme critério do SINE-IDT/CE;

7.5.7.7 O controle de acesso deve permitir a configuração de acesso por perfil às funções de Administração, Incidentes, Configuração de Regras, acesso a atividades de Redes e Logs;

7.5.7.8 Permitir visualização de eventos, flows de rede e incidentes de segurança em tempo próximo ao real;

7.5.7.9 Permitir pesquisa nos eventos históricos, a partir de metadados, fornecendo capacidade de "drill-down", ou seja, o refinamento da pesquisa a partir da seleção de elementos no resultado, para efetuar nova pesquisa.

7.5.7.10 Deve permitir a visualização dos detalhes dos eventos, inclusive o evento original ("raw"), quando aplicável, para análise forense e investigação de incidentes;

7.5.7.11 Permitir a visualização dos eventos relacionados a um alerta e/ou incidente de segurança identificado pelas regras de correlação da solução;

7.5.7.12 Capacidade de criação de novos painéis gráficos (dashboards) e alteração dos existentes;

7.5.7.13 Capacidade de visualizar eventos de mais de um tipo de dispositivo na mesma visualização (ex: Firewall, Proxy e anti-vírus na mesma visualização);

7.5.7.14 Permitir a criação de novos modelos de relatórios e alteração dos relatórios nativos da solução sem a necessidade de uso de linguagens de programação, através da interface web;

7.5.7.15 Permitir agendar a geração de relatórios de forma periódica e notificar/enviar automaticamente os relatórios gerados para os destinatários dos mesmos;

7.5.7.16 Capacidade de criação de listas (watchlist) e alteração das existentes. Permitindo a inserção dos dados de forma manual, por linha de comando e automática através das regras de correlação;

7.5.7.17 Permitir a remoção de dados das listas (watchlist) de forma manual e pela expiração do tempo de vida da informação;

7.5.7.18 Capacidade de gerenciamento e configuração centralizada de todas as partes distribuídas da solução;

7.5.7.19 Capacidade de atualização de componentes da solução, a partir da console central de administração;

7.5.7.20 Capacidade de restaurar informações de cópia de segurança do banco de dados, configurações e dados, que foram arquivadas previamente pela solução;

7.5.7.21 Permitir a criação de novos tipos de eventos na ferramenta, a fim de integrar logs não suportados nativamente;

7.5.7.22 Permitir a associação manual de eventos já normalizados, mas ainda não categorizados/associados, às categorias, classificações ou tipos de eventos já existentes, ou aos definidos pelo usuário;

7.5.7.23 Para análise dos eventos e flows de rede, deve suportar buscas e filtros de eventos, usando filtros simples (ex: IP = 10.10.10.10) e buscas avançadas, utilizando sintaxe SQL ou similar;

7.5.7.24 Deve disponibilizar APIs do tipo webservices, do tipo "RESTful API", para acesso externo à solução, permitindo busca de informações de eventos e flows, manipulação de incidentes.

7.5.7.25 Deve possuir dashboard sumarizado com dados de conformidade;

7.5.7.26 Deve possuir templates de relatórios para as principais normas de conformidade. Sendo exigido, no mínimo, o atendimento a ISO-27001, PCI, e SOX;

7.5.7.27 Deve suportar o controle de acesso a solução baseado em informações externas a solução, através da validação de atributo do usuário ou grupo que esse faz parte. Deve suportar essa validação de autorização em diretórios LDAP ou Windows Active Directory.

7.5.8 Tratamento de Incidentes

7.5.8.1 Possuir ferramenta interna para o de tratamento dos incidentes identificados pelas regras de correlação;

7.5.8.2 Permitir associar os incidentes aos usuários da solução;

7.5.8.3 Permitir encerrar um incidente quando este for solucionado;

7.5.8.4 Permitir adicionar anotações aos incidentes para registro das ações tomadas ou observações;

7.5.8.5 Permitir a integração com ferramentas de tratamento de incidentes externos, nativamente ou possuir recursos como envio de Trap SNMP, Syslog e mensagens SMTP a partir da geração de um incidente, permitindo a manipulação do incidente por RESTful API.

7.5.9 Compatibilidade e escalabilidade

7.5.9.1 A Solução deve ser capaz de coletar e interpretar logs de diferentes ativos de rede, segurança e informação do ambiente.

7.5.9.2 Se necessário, a solução poderá distribuir os componentes da solução em diferentes equipamentos, para melhor desempenho ou funcionalidade;

7.5.9.3 O componente de coleta de eventos deve suportar a recepção, a normalização, e o tratamento de eventos/logs em tempo próximo ao real (near real-time);

7.5.9.4 Deve ter a capacidade para suportar a adição de novos componentes para garantir a escalabilidade, inclusive referente ao banco de dados;

7.5.9.5 Os ativos indicados abaixo devem ser suportados pela solução, os quais poderão ter suporte nativo ou por meio de customização para coleta dos logs e correlação:

7.5.9.5.1 Firewall

7.5.9.5.1.1 Checkpoint;

7.5.9.5.1.2 PIX Firewall;

7.5.9.5.1.3 Fortinet Fortigate;

7.5.9.5.1.4 Palo Alto Networks;

7.5.9.5.1.5 IPTables;

7.5.9.5.1.6 Detecção/Prevenção de Intrusos

7.5.9.5.1.7 Tipping Point;

7.5.9.5.1.8 Sourcefire Defense Center;

7.5.9.5.1.9 Snort;

7.5.9.5.1.10 Cisco IPS;

7.5.9.5.1.11 IBM NIPS GX e XGS;

7.5.9.5.1.12 McAfee;

7.5.9.5.2 Antivirus/Antimalware

7.5.9.5.2.1 Trend Micro;

7.5.9.5.2.2 Symantec System Center;

7.5.9.5.2.3 Symantec Endpoint Protection;

7.5.9.5.2.4 McAfee ePolicy Orchestrator (ePO);
7.5.9.5.2.5 Kaspersky Security Center;
7.5.9.5.2.6 FireEye;
7.5.9.5.3 Sistemas Operacionais
7.5.9.5.3.1 Linux;
7.5.9.5.3.2 Microsoft Windows;
7.5.9.5.3.3 IBM AIX;
7.5.9.5.3.4 IBM zOS;
7.5.9.5.3.5 IBM AS400;
7.5.9.5.3.6 HP-UX;
7.5.9.5.3.7 Sun Solaris;
7.5.9.5.4 Servidor Web
7.5.9.5.4.1 Microsoft IIS;
7.5.9.5.4.2 Apache;
7.5.9.5.5 Servidor Proxy;
7.5.9.5.5.1 Squid Web Proxy;
7.5.9.5.5.2 BlueCoat SG;
7.5.9.5.5.3 IronPort Security Web Security;
7.5.9.5.5.4 Websense
7.5.9.5.5.5 McAfee Web Gateway;
7.5.9.5.6 Roteadores/switches
7.5.9.5.6.1 3com;
7.5.9.5.6.2 Nortel;
7.5.9.5.6.3 Extreme;
7.5.9.5.6.4 Enterasys;
7.5.9.5.6.5 Cisco;
7.5.9.5.6.6 Juniper;
7.5.9.5.7 Servidor de Banco de dados
7.5.9.5.7.1 Oracle;
7.5.9.5.7.2 Microsoft SQL;
7.5.9.5.7.3 DB2;
7.5.9.5.8 Syslog em geral;
7.5.9.5.9 Scanners de vulnerabilidades
7.5.9.5.9.1 Nessus;
7.5.9.5.9.2 QualysQuard;
7.5.9.5.9.3 Foundstone;
7.5.9.5.9.4 NMAP;
7.5.9.5.10 Concentrador VPN;
7.5.9.5.10.1 NORTEL;
7.5.9.5.10.2 Check Point UTM;
7.5.9.5.10.3 Cisco;

7.5.10 Relatórios

7.5.10.1 A solução deve apresentar, no mínimo as seguintes características relacionadas a geração de relatórios;

7.5.10.2 Deve permitir a geração de relatórios, contendo múltiplas informações num mesmo relatório, como dados de segurança e rede;

7.5.10.3 Deve implementar nativamente relatórios de conformidade com normas reguladoras do mercado, no mínimo: SOX, PCI 2.0 e ISO-27001;

7.5.10.4 Deve permitir a criação de relatórios relacionados a: incidentes, logs, flows de rede, vulnerabilidades;

7.5.10.5 Deve possuir relatórios classificados em grupos temáticos, permitindo a criação novos agrupamentos de relatórios pelo usuário;

7.5.10.6 Deve permitir a customização de novos relatórios baseados em dados de Logs, Flows de rede, Vulnerabilidades e Incidentes;

7.5.10.7 Deve gerar relatórios de eventos, alertas/incidentes em nível técnico e gerencial os quais devem ter a possibilidade de serem gerados em PDF, HTML, XLS, XML e RTF/DOC;

7.5.10.8 Permitir o agendamento de relatórios de forma periódica e notificar/enviar automaticamente por e-mail os relatórios gerados para os destinatários dos mesmos;

7.5.10.9 Os usuários devem poder visualizar apenas os seus próprios relatórios ou relatórios disponibilizados por outros usuários, os administradores devem poder visualizar todos os relatórios;

7.5.10.10 Deve ser possível definir perfis de usuários com permissão/restrição de edição dos modelos de relatórios;

7.5.10.11 Deve ser possível realizar relatórios baseados em dados com IPv6;

7.5.10.12 A funcionalidade de cópia de segurança deve preservar os dados de relatórios;

7.5.10.13 Deve ser possível alterar ou adicionar a logomarca do relatório para customização;

7.5.10.14 Os relatórios nativos da solução devem poder ser editados e duplicados para novos relatórios.

8 SLA (ACORDO DE NÍVEL DE SERVIÇO)

8.1 Os tempos máximos de atendimento especificados nas tabelas abaixo devem ser seguidos, sob pena de multa prevista neste edital:

Atividade	Tempo de Resposta Máximo
Alteração e inclusão de regras	240 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Alteração de configurações	240 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Atualização (implementação de patches e fixes)	48 horas após liberação do pacote pelo fabricante, condicionado à homologação pela Contratada e liberação de janela de mudança pelo SINE-IDT/CE.
Início de atuação remota para resolução de problemas	120 minutos após abertura de chamado ou detecção pelo SNOC.

Atividade	Tempo de Resposta Máximo
Substituição ou troca de equipamentos imediatos	**Em até 24 horas uteis após abertura de chamado da Contratante**.
Implementação de novos serviços ou dispositivos (VPN, placas de rede, etc.)	24 horas após abertura de chamado.
Relatório Periódico Técnico	Mensal.
Relatório emergencial	24 horas após o evento, desde que solicitado pelo SINE-IDT/CE.

Tabela 1 - SLA para serviço

8.2 Em casos emergenciais, quando houver a paralização nas atividades do negócio ou uma demanda de nível superior, o SINE-IDT/CE poderá abrir chamados emergenciais, com o SLA diferenciado, conforme tabela chamados emergenciais. Poderão ser abertos, no máximo, 2 (dois) chamados emergenciais por mês.

8.2.1 Chamada Emergencial

Atividade	Tempo de Resposta 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.
Alteração e inclusão de assinaturas de reconhecimento de ataques	60 minutos após a liberação do pacote de assinaturas pelo fabricante, condicionado à homologação pela Contratada.
Alteração de configurações	60 minutos após abertura de chamado, exceto quando for necessária uma janela de manutenção.
Início de atuação remota para resolução de problemas	60 minutos após abertura de chamado.

Tabela 2 - SLA para Serviços Emergenciais

8.3 Os SLAs, especificados nos itens 1 a 3, poderão vir a ser revisados somente após decorridos um mínimo de1 (um) ano após a assinatura do Contrato, caso o SINE-IDT/CE entenda que os tempos aqui especificados não estariam atendendo às suas necessidades, sujeito à aceitação pela Contratada.

9 VISITA TÉCNICA

9.1 Para que a empresa Licitante possa compreender a complexidade do ambiente tecnológico do SINE-IDT/CE, **é aconselhável a realização de Visita Técnica ao ambiente de TI em até 4 (quatro) dias úteis antes da data de abertura das propostas.**

9.2 A Visita Técnica deverá ser realizada por um representante devidamente credenciado da empresa Licitante ou por procurador, devidamente autorizado através de procuração pública para tanto.

10 COMPROVAÇÕES PARA FINS DE HABILITAÇÃO

10.1 Todos os documentos solicitados devem ser apresentados em original ou sua cópia autenticada em cartório.

10.2 Para fins de Habilitação serão exigidas as seguintes comprovações técnicas:

10.2.1 Original ou cópia autenticada das declarações conferidas por empresas públicas ou privadas, para fins de comprovação do item 5.4.1 deste Termo de Referência.

10.2.2 Declaração dos fabricantes das soluções abaixo definidas, emitida especificamente para o SINE-IDT/CE e referente a esse processo licitatório, em papel timbrado e devidamente assinado, informando que é revenda autorizada pelo mesmo assim como estando capacitada para implementar suas soluções e especificando-as.

10.2.2.1 Firewall UTM (Antivírus/Antispyware de Gateway, IDS/IPS e VPN).

10.2.2.2 Rede Wireless Segura.

10.2.2.3 Filtro de Conteúdo Web.

11 REQUISITOS OBRIGATÓRIOS GERAIS

11.1 Todas as características técnicas relativas aos produtos e serviços exigidas na especificação das soluções técnicas deverão ser comprovadas, independente da descrição da proposta, através de documentos cujas origens sejam exclusivamente o fabricante dos equipamentos, como catálogos, manuais ou ficha de especificação técnica, sob a forma de volumes impressos ou em meio eletrônico (CD, DVD, etc.). **A não comprovação de alguma/ qualquer característica/ funcionalidade/ exigência aqui especificada levará a desclassificação imediata da Licitante.**

11.1.1 Serão aceitas declarações de fabricantes para itens que não possuam documentação divulgada, de preferência com referência a manuais, páginas de Internet ou telas dos produtos, **desde que tal funcionalidade seja comprovada através de demonstração presencial para a equipe do SINE-IDT/CE que atestará sobre o funcionamento ou não dos itens que retratarem as funcionalidades requeridas, sob pena de imediata desclassificação da Licitante decorrente e não comprovação**.

11.2 As informações obtidas em sites oficiais dos fabricantes através da Internet deverão ser impressas e anexadas à proposta e deverá ser indicado à respectiva URL (Uniform Resource Locator) onde se encontram.

11.3 Serão aceitos documentos em português ou inglês para comprovações técnicas.

11.4 Caso seja fornecida em meio eletrônico, a documentação técnica deverá estar em formato amplamente utilizado (Microsoft WORD, PDF, HTML, CHM) ou ser acompanhada de recurso adequado para visualização na tela e impressão em papel no tamanho A4. A documentação técnica deverá apresentar-se perfeitamente legível, sendo os detalhes das figuras facilmente reconhecíveis.

12 LOCAL DE IMPLANTAÇÃO DOS SERVIÇOS

12.1 A instalação dos equipamentos e sistemas que permitirão a prestação dos serviços de que trata este Termo de Referência será nas localidades descritas no Anexo.

12.2 Caberá à Contratada, arcar com quaisquer custos de deslocamento, hospedagem, alimentação ou outro qualquer, pois os mesmos já devem estar contemplados no valor dos serviços de implantação.

13 CONDIÇÕES DE ENTREGA E IMPLANTAÇÃO DOS SERVIÇOS

13.1 O SINE-IDT/CE solicitará a implantação dos serviços adjudicados por meio de AES - Autorização de Execução de Serviço que contemplará o nome dos serviços a serem implantados.

13.2 O prazo para entrega dos equipamentos que comporão os serviços a serem prestados pela Contratada será de 30 (trinta) dias consecutivos, contados a partir da data da emissão das Solicitações de Serviços pelo SINE-IDT/CE.

13.3 Os equipamentos e sistemas que compõem os serviços deverão ser entregues e instalados no SINE-IDT/CE. As fases da implantação dos serviços devem contemplar:

13.3.1 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 SINE-IDT/CE, bem como quaisquer outros itens que sejam necessários para a implantação do projeto. Deve se considerar as janelas de manutenção do SINE-IDT/CE, plano de rollback e o escopo definido. Os responsáveis técnicos do SINE-IDT/CE acompanharão e aprovarão o planejamento.

13.3.1.1 O prazo para a implantação de cada uma das soluções e dos serviços requeridas, pela Contratada, estará devidamente especificado na tabela abaixo. O prazo será contado a partir da data acordada entre o SINE-IDT/CE e a Contratada para implantação do serviço, com aceite oficial do SINE-IDT/CE, após a data de recebimento dos equipamentos no SINE-IDT/CE:

Serviço	**Tempo Máximo de Implantação (Dias Corridos)**
Serviço de Firewall UTM	15 (quinze) dias.
Serviço de Rede Wireless	15 (quinze) dias
Serviço de Backup;	15 (quinze) dias
Serviço de Filtro Web	15 (quinze) dias
Serviço de Correlacionamento de Eventos	15 (quinze) dias

Tabela: Prazo para Implantação dos Serviços por Categoria

13.3.2 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 visando tornar o ambiente mais seguro e controlado, quanto à confidencialidade, integridade e disponibilidade do ambiente.

13.3.3 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.

13.3.4 Homologação: Após a conclusão dos testes, as soluções deverão ser formalmente homologadas pelo SINE-IDT/CE, com a finalidade de iniciar a monitoração, operação dos serviços e gerenciamento do ambiente, dentro do SLA especificado.

13.3.4.1 O SINE-IDT/CE terá o prazo de 15 (quinze) dias consecutivos, contados a partir da data de conclusão dos serviços de instalação e configuração dos serviços contratados, para emitir o relatório de homologação (aceite).

13.3.4.2 Os serviços serão aceitos 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.

13.3.5 Documentação: A Contratada deverá elaborar e manter atualizada a documentação das atividades e de todos os processos que ocorrerão.

13.3.5.1 Devem ser documentados: a entrega e conferência, testes, homologação, compromissos e prazos, incluindo planos de trabalho, planos de contingência, cronogramas, atas de reuniões, de modo a compor documentação ("as built") a ser entregue ao SINE-IDT/CE ao final da implantação. O SINE-IDT/CE poderá propor atualizações nesse documento, no sentido de melhor atender ao bom andamento dos trabalhos ou à sua própria conveniência.

13.3.5.2 Com a finalização da etapa de testes e homologação deverá ser realizada uma apresentação *in loco*, com a finalidade de registrar as intervenções realizadas no ambiente ativo atual, apresentar a metodologia do serviço gerenciado ao SINE-IDT/CE, formalizar o Plano de Comunicação, formatar a Matriz de Responsabilidades (com os nomes e pessoas chave responsáveis) e ratificar o SLA da solução contratada.

14 VALOR DOS SERVIÇOS

14.1. A tarifação dos serviços compreenderá os seguintes valores, a serem expressos em R$ (reais), conforme Anexo I:

14.1.1. O Total Geral de Custos do Contrato, para 12 (doze) meses de prestação dos serviços contratados, será o valor a ser utilizado como base para os lances do certame. Este valor será composto pela soma das mensalidades de todos os serviços, considerando-se 12 (doze) meses de período contratual.

14.1.2. O valor da instalação realizado uma única vez deve incluir o planejamento, implantação e testes de todas as funcionalidades e estar orçado na composição do valor unitário do serviço.

15. DO PAGAMENTO

15.1. O pagamento será efetuado até 10 (dez) dias contados da data da apresentação da Nota Fiscal e Recibo, devidamente atestada pelo gestor da contratação, acompanhada da Autorização de Serviço e da Documentação relativa à regularidade para com a Seguridade Social (INSS), Fundo de Garantia por Tempo de Serviço (FGTS),Trabalhista e Fazendas Federal, Estadual e Municipal, mediante emissão de cheque nominal ou depósito em conta bancária.

15.2. A nota fiscal/fatura que apresente incorreções será devolvida à CONTRATADA para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

15.3. Não será efetuado qualquer pagamento à CONTRATADA**,** em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

15.4. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.

15.5. Caso ocorra, a qualquer tempo, a não aceitação de qualquer parte do fornecimento, o prazo de pagamento será interrompido e reiniciado após a correção pela CONTRATADA.

15.6. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em Cartório. Caso a documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

16. DAS SANÇÕES ADMINISTRATIVAS

16.1. O licitante que praticar quaisquer das condutas previstas no art. 32, do Decreto Estadual nº 28.089/2006, sem prejuízo das sanções legais nas esferas civil e criminal, estará sujeito às seguintes penalidades:

16.1.1. Multa de 10% (dez por cento) sobre o valor da proposta.

16.1.2. Impedimento de licitar e contratar com o Instituto de Desenvolvimento do Trabalho - IDT, sendo, então, descredenciado no cadastro de fornecedores, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste edital e das demais cominações legais.

16.2. O licitante recolherá a multa por meio de Pagamento na Tesouraria do IDT podendo ser substituído por outro instrumento legal, em nome do órgão Contratante. Se não o fizer, será cobrada em processo de execução.

16.2.1. O atraso injustificado no prazo de fornecimento implicará multa correspondente a 3,33% (três vírgula trinta e três por cento) por dia, calculada sobre o valor total do contrato ou da parcela dos serviços não cumprida, até o limite de **10%** (dez por cento) desse valor.

16.2.2. Na hipótese mencionada no item anterior, o atraso injustificado por período **superior a 05(cinco) dias** caracterizará o descumprimento total da obrigação, punível com a rescisão unilateral do contrato e suas conseqüências, e da aplicação da sanção prevista no item 16.01.02.

16.2.3. As multas porventura aplicadas serão descontadas dos pagamentos devidos pela Contratante ou cobradas diretamente da Contratada, administrativa ou judicialmente, e poderão ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

16.2.4. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério da Contratante.

16.2.5. Sempre que não houver prejuízo para a Contratante, as penalidades impostas poderão ser relevadas ou transformadas em outras de menor sanção, a seu critério.

16.2.6. As aplicações das penalidades serão precedidas de concessões de oportunidades de ampla defesa por parte da Contratada, na forma da lei.

17. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATADA

17.1. Assegurar-se que o local de instalação dos equipamentos necessários à Prestação dos Serviços neste edital precificada possui as condições técnicas e ambientas necessárias ao pleno, seguro e normal funcionamento dos equipamentos necessários à prestação dos serviços.

17.2. Especificar e requerer do SINE-IDT/CE as condições técnicas e ambientais para a instalação das Soluções em no máximo 48 (quarenta e oito) horas úteis do recebimento da Solicitação de Serviço para implantação das soluções e serviços contratados.

17.3. Manter os Centros de Operação de Segurança e Rede (SNOC) próprios para monitoramento remoto 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), com infra-estrutura estritamente de acordo com as especificações deste documento.

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

17.5. Responsabilizar-se pela manutenção preventiva e corretiva dos hardwares e softwares por ela ofertados.

17.5.1. **Todas as soluções de hardwares e softwares, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de locação.**

17.6. Iniciar a Prestação dos Serviços rigorosamente em estrita observância aos prazos estabelecidos neste Termo de Referência.

17.7. Implementar/gerenciar o backup de configuração de sistemas (regras) e análise de logs.

17.8. Realizar qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de "patches" e correlatos.) mediante autorização formal do SINE-IDT/CE.

17.9. Comunicar, imediatamente, a eminência ou ocorrência de 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 SINE-IDT/CE.

17.10. Responsabilizar-se integralmente por todas as implantações das soluções.

17.11. Resolver os chamados de Serviço e Suporte Técnico conforme os tempos definidos nas tabelas de tempos de atendimento (SLA) deste Termo de Referência.

17.11.1. A substituição de Equipamentos com Defeito, que cause a Indisponibilidade de Serviço fica direta e estritamente vinculada em conformidade com o tempo estipulado na Tabela de Tempos de Atendimento (SLA).

17.12. Manter os Serviços contratados em cumprimento aos Níveis de Disponibilidade estabelecidos em item 06 deste Termo de Referência.

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

17.13. Responsabilizar-se por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do SINE-IDT/CE, sem prejuízo aos serviços desta.

17.14. 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 SLA estabelecido neste Termo de Referência.

17.15. Produzir e enviar por e-mail, mensalmente, relatórios analíticos a equipe gestora do SINE-IDT/CE, ou em 24 (vinte e quatro) horas quando houver demanda.

17.16. **Participar, mensalmente, de reuniões presenciais**, de ponto de controle, para apresentação dos indicadores de disponibilidade, diagnósticos dos ambientes monitorados, dirimir dúvidas sobre os serviços contratados, análise e entendimento dos relatórios gerenciais e administrativos, revisão das configurações e procedimentos implementados e melhorias a serem implementadas.

17.17. 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 SINE-IDT/CE, praticado por seus empregados, conforme **TERMO DE CONFIDENCIALIDADE – ANEXO VII**, a ser assinado pela Contratada no ato da assinatura do Contrato.

18. OBRIGAÇÕES E RESPONSABILIDADES DA CONTRATANTE

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

18.1. 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 que se tornem necessárias.

18.2. Informar aos técnicos da Contratada as necessidades de configuração dos equipamentos e serviços, por meio da abertura de chamados de suporte técnico, e quando necessário, podem ser anexados aos chamados arquivos com as necessidades de configurações.

18.3. Cumprir pontualmente todos os seus compromissos financeiros para com a Contratada.

18.4. 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.

18.5. Comunicar à Contratada todas as possíveis irregularidades detectadas na execução dos serviços contratados.

18.6. Fiscalizar e acompanhar a execução dos serviços de que trata o objeto deste Termo de Referência.

18.6.1. Atestar a sua prestação se, e somente se, os serviços executados atenderem plenamente às especificações constantes deste Termo de Referência.

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

18.6.2.1. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada pelos danos causados ao SINE-IDT/CE ou a Terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos.

19. DA VIGENCIA DO REGISTRO DE PREÇOS

19.1. A Ata de Registro de Preços terá validade pelo prazo de 12 (doze) meses, contado a partir da data da sua publicação.

20. DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

20.1 Os contratos terão prazo de vigência de até 12(doze) meses contados a partir da data de sua assinatura, podendo, no interesse da administração, mediante Termo Aditivo, ser prorrogado por iguais e sucessivos períodos, limitada a sua duração a 60 (sessenta) meses, "ex-vi" do disposto no Inciso II, do Artigo 57, da Lei nº 8.666/93.

.

Viliberto Cavalcante Porto Júnior
Gerente da Célula de Tecnologia da Informação

ANEXO II

PROPOSTA COMERCIAL

(Modelo - Utilizar papel timbrado da instituição).

Ref.: PREGÃO ELETRÔNICO Nº _____/20_____ - IDT

1. **Identificação do Licitante:**
    - Razão Social:
    - CPF/CNPJ e Inscrição Estadual
    - Endereço completo
    - Representante Legal (nome, nacionalidade, estado civil, profissão, CPF, domicílio)
    - Telefone, celular, fax, e-mail
    - Banco, Agência e nº da Conta Corrente
2. **Condições Gerais da Proposta:**
    a) A presente proposta é válida por 60 (sessenta) dias, contados da data de sua emissão.
3. **Formação do Preço:**

Lote Nº 1

Item	Descrição	Quant./ mês	Quant. /ano	Valor unitário (R$)	Valor Total/ano (R$)
a.i)	Serviço de Firewall UTM e aqui denominado Médio e Grande Porte – Tipo I	1	12		
a.ii)	Serviço de Firewall UTM aqui denominado de Pequeno Porte – Tipo II	100	1200		
b)	Serviços de Rede Wireless Segura	20	240		
c)	Serviço de Backup	1	12		
d)	Serviço de Filtro Web	1	12		
e)	Serviço de Correlação de Eventos	1	12		
VALOR TOTAL DA PROPOSTA					**R$**

Obs: O valor estimado da instalação deverá estar incluso no valor unitário dos serviços.

Local e Data
RG e Assinatura do Representante Legal
(Nome e Cargo)

ANEXO II-A

LISTA DAS LOCALIDADES E ENDEREÇO DAS UNIDADES SINE-IDT/CE

Tendo em vista a necessidade de instalação futura de nova(s) unidade(s) fica desde já esclarecido/precificado que a Licitante Vencedora poderá ter que implementar os serviços e soluções objeto desta contratação na(s) nova(s) localidade(s) e seu(s) respectivo(s) endereço(s) a mediada que vier(em) a ocorrer em conformidade com tudo que neste edital se aplicar ao assunto.

ITEM	UNIDADES DE ATENDIMENTO	ENDEREÇO	VELOCIDADE EM Mbps	TIPO DE ACESSO	ESTAÇÕES DE REDE
FORTALEZA E RMF					
1.	SEDE DO IDT	Av. Universidade, 2596, Benfica - Fortaleza/CE - CEP: 60.020-180	100	FIBRA ÓPTICA	362
2.	DATA CENTER (link de comunicação com storage backup)	Av. Santos Dumont, 2626 salas 19 e 20 - Aldeota - Fortaleza/CE - CEP 60.150-161	20	FIBRA ÓPTICA	-
3.	SNOC (monitoramento dos firewalls)	Rua Desembargador Leite Albuquerque, 816, 3º andar - Fortaleza/CE - CEP: 60.150-150	5	FIBRA ÓPTICA	-
4.	UNIDADE DE ATENDIMENTO DA ALDEOTA	Av. Santos Dumont, 5015, Aldeota - Fortaleza/CE - CEP: 60.150-162	5	FIBRA ÓPTICA	17
5.	UNIDADE DE ATENDIMENTO AQUIRAZ	Rua Capitão Mor, 37, Centro - Aquiraz/CE CEP: 61.700-000	5	FIBRA ÓPTICA	8
6.	UNIDADE DE ATENDIMENTO DA BARRA DO CEARA	Av. Francisco Sá, 6485, Barra do Ceará - Fortaleza/CE - CEP: 60.330-875	5	FIBRA ÓPTICA	16
7.	UNIDADE DE ATENDIMENTO	Rua Juaci Sampaio Ponte, 2076, Centro - Caucaia/CE -	5	FIBRA ÓPTICA	11

	DA CAUCAIA	CEP: 61.600-150			
8.	UNIDADE DE ATENDIMENTO DE CASCAVEL	Av. Dr. Pedro de Queiroz Ferreira, 1891 - Centro - Cascavel/CE - CEP: 62.850-000	5	FIBRA ÓPTICA	7
9.	UNIDADE DE ATENDIMENTO DO CENTRO	Rua Assunção, 699, Centro - Fortaleza/CE – CEP: 60.840-045	5	FIBRA ÓPTICA	67
10.	UNIDADE DE ATENDIMENTO DO CTA	Rua Floriano Peixoto, 1375, Centro - Fortaleza/CE - CEP: 60.025-131	5	FIBRA ÓPTICA	15
11.	UNIDADE DE ATENDIMENTO DO EUSÉBIO	Rua Irmã Ambrosina, 83, Centro – Eusébio/CE - CEP: 61.760-000	5	FIBRA ÓPTICA	6
12.	UNIDADE DE ATENDIMENTO HORIZONTE	Av. Pres. Castelo Branco, 4591, Centro - Horizonte/CE - CEP: 62.880-000	5	FIBRA ÓPTICA	9
13.	UNIDADE DE ATENDIMENTO DE MARACANAU	Av. Do Contorno, 615, 1º Distrito Industrial - Maracanaú/CE – CEP: 61.939-160	5	FIBRA ÓPTICA	18
14.	UNIDADE DE ATENDIMENTO MARANGUAPE	Rua Mundica Paula, 216, Centro - Maranguape/CE - CEP: 61.940-145	5	FIBRA ÓPTICA	9

15.	UNIDADE DE ATENDIMENTO MESSEJANA	Rua Dr. Pergentino Maia 813 A, Messejana - Fortaleza/CE - CEP: 60.840-110	5	FIBRA ÓPTICA	25
16.	UNIDADE DE ATENDIMENTO DE PACAJUS	Rua Luis Claudio, S/N, Centro - Pacajus/CE - CEP: 62.870-000	5	FIBRA ÓPTICA	8
17.	UNIDADE DE ATENDIMENTO DE PACATUBA	Rua Coronel José Libânio, 412 C, Centro - Pacatuba/CE - CEP: 61.800-000	5	FIBRA ÓPTICA	8
18.	UNIDADE DE ATENDIMENTO DA PARANGABA	Av. João Pessoa, 6239, Parangaba - Fortaleza/CE - CEP: 60.435-682	5	FIBRA ÓPTICA	33
19.	UNIDADE DE ATENDIMENTO PECÉM	Rua Francisco Câncio, S/N, Pecém - São Gonçalo do Amarante/CE - CEP: 62.674-000	5	FIBRA ÓPTICA	11
20.	BALCÃO DE EMPREGO CDL	Rua 25 de Março, 882 - Centro - Fortaleza/CE - CEP: 60.001-970	5	FIBRA ÓPTICA	2
21.	BALCÃO DE EMPREGO DO SHOPPING BENFICA	Av. Carapinima, 2200, Benfica - Fortaleza/CE - CEP: 60.015-220	5	FIBRA ÓPTICA	3
22.	BALCÃO DE EMPREGO DO SHOPPING DIOGO	Rua Barão do Rio Branco, 2059, 1º andar - Shopping Diogo, Centro - Fortaleza/CE – CEP: 60.025-903	5	FIBRA ÓPTICA	3

INTERIOR					
23.	UNIDADE DE ATENDIMENTO DE ARACATI	Rua Cel. Alexanzito, 447, Centro - CEP: 62.800-000	5	FIBRA ÓPTICA	8
24.	UNIDADE DE ATENDIMENTO DE BARBALHA	Rua dos Carris, 12, Centro - Barbalha/CE - CEP: 63.180-000	5	FIBRA ÓPTICA	6
25.	UNIDADE DE ATENDIMENTO DE BATURITÉ	Av. Francisco Braga Filho, 1015, Conselheiro Estelita - Baturité/CE - CEP: 62.760-000	5	FIBRA ÓPTICA	4
26.	UNIDADE DE ATENDIMENTO DE CAMOCIM	Rua Paissandu, 1801, Centro - Camocim/CE- CEP: 62.400-000	5	FIBRA ÓPTICA	8
27.	UNIDADE DE ATENDIMENTO CANINDÉ	Praça Nem Martins, 2164, Centro - Canindé/CE - CEP: 62.700-000	5	FIBRA ÓPTICA	6
28.	UNIDADE DE ATENDIMENTO DE CRATEÚS	Rua Coronel Zezé, 1216, Centro - Crateús/CE - CEP: 63.700-000	5	FIBRA ÓPTICA	8
29.	UNIDADE DE ATENDIMENTO DO CRATO	Rua Monsenhor Esmeraldo, 686, Centro - Crato/CE - CEP: 63.100-000	5	FIBRA ÓPTICA	8
30.	UNIDADE DE ATENDIMENTO IGUATÚ	Rua Cel. Gustavo Correia, 171, Centro -Iguatu/CE - CEP: 63.500-029	5	FIBRA ÓPTICA	9
31.	UNIDADE DE ATENDIMENTO DE ITAPIPOCA	Rua Mons. Tabosa, 2989, Coqueiro - Itapipoca/CE – CEP: 62.500-000	5	FIBRA ÓPTICA	7
32.	UNIDADE DE	Rua José Marrocos,	5	FIBRA	

	ATENDIMENTO JUAZEIRO DO NORTE	S/N, Santa Tereza - Juazeiro do Norte/CE - CEP: 63.050-240		ÓPTICA	12
33.	UNIDADE DE ATENDIMENTO DE LIMOEIRO DO NORTE	Rua José Satino, 120, Centro - Limoeiro do Norte/CE - CEP: 62.930-000	5	FIBRA ÓPTICA	9
34.	UNIDADE DE ATENDIMENTO DE MORADA NOVA	Av. Manoel Castro de Andrade, 301, Centro - Morada Nova/CE - CEP: 62.940-000	5	FIBRA ÓPTICA	5
35.	UNIDADE DE ATENDIMENTO QUIXADÁ	Rua Dr. Rui Maia, 420, Centro - Quixadá/CE - CEP: 63.900-970	5	FIBRA ÓPTICA	10
36.	UNIDADE DE ATENDIMENTO QUIXERAMOBIM	Rua: Dona Francisca Santiago, 30, Centro - Quixeramobim/CE - CEP: 63.800-000	5	FIBRA ÓPTICA	7
37.	UNIDADE DE ATENDIMENTO DE RUSSAS	Rua Cel. Araújo Lima, 1458 A, Centro - Russas/CE - CEP: 62.900-000	5	FIBRA ÓPTICA	9
38.	UNIDADE DE ATENDIMENTO DE SOBRAL	Rua Paulo Aragão, 659, Centro - Sobral/CE - CEP: 62.011-250	5	FIBRA ÓPTICA	19
39.	UNIDADE DE ATENDIMENTO TAUÁ	Av. Odilon Aguiar, 19 - Centro - Tauá/CE - CEP: 63.660-000	5	FIBRA ÓPTICA	5
40.	UNIDADE DE ATENDIMENTO DE TIANGUA	Av. Prefeito Jaques Nunes, 1.411, Centro - Tiangua/CE - CEP: 62.320-000	5	FIBRA ÓPTICA	4

41.	UNIDADE DE ATENDIMENTO DE UBAJARA	Rua Esmerino Magalhães, 214, Centro - Ubajara/CE - CEP: 62.350-000	5	FIBRA ÓPTICA	8
PROJOVEM					
42.	SEDE DO PROJOVEM	Av. Universidade, 2567, Benfica - Fortaleza/CE - CEP: 60.020-180	1.024	FIBRA ÓPTICA	46
43.	POLO DE QUIXERAMOBIM	Rua Desembargador Américo Militão, 361, Centro - Quixeramobim/CE - CEP: 60.800-000	5	FIBRA ÓPTICA	8
44.	POLO DE TIANGUA	Rua Teófilo Ramos, 397, Centro - Tianguá/CE - CEP: 62.320-000	5	FIBRA ÓPTICA	13

ANEXO III

DECLARAÇÃO ESPECIAL

(Utilizar papel timbrado da instituição).

Ao
INSTITUTO DE DESENVOLVIMENTO DO TRABALHO – IDT
Av. da Universidade, 2596 – Benfica – Fortaleza/CE

PREGÃO ELETRÔNICO N.º ____/20__

A empresa ....., inscrito no CNPJ n.º ....., por intermédio de seu representante legal o (a) Sr (a) ....., portador (a) da Carteira de Identidade n.º ..... e do CPF n.º ..... DECLARA, para fins desta licitação:

a) que recebeu e estudou todos os documentos inerentes à presente competição e tomado conhecimento integral do teor do edital de licitação supracitado, sujeitando-se às disposições nele contidas;

b) que não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e que não emprega menores de 16 (dezesseis) anos, salvo se na condição de aprendiz, a partir dos 14 (quatorze) anos;

c) que não está suspensa do direito de licitar e que não foi declarada inidônea para licitar ou contratar com a Administração Pública e/ou com o Instituto de Desenvolvimento do Trabalho -IDT, bem como comunicará qualquer fato ou evento superveniente quanto à habilitação ao certame supra;

d) que na composição societária não existe participação de dirigentes ou empregados da entidade promotora da licitação.

Concorda e submete-se a todas e cada uma das condições impostas pelo referido edital.

Data e local

Assinatura/identificação do nome
RG e cargo do representante legal da LICITANTE

ANEXO IV

DADOS DA EMPRESA E REPRESENTANTE LEGAL

(Utilizar papel timbrado da instituição).

Ao
INSTITUTO DE DESENVOLVIMENTO DO TRABALHO – IDT
Av. da Universidade, 2596 – Benfica – Fortaleza/CE
AO: INSTITUTO DE DESENVOLVIMENTO DO TRABALHO – IDT

PREGÃO ELETRÔNICO Nº _____/20____

Razão Social: _____CNPJ/MF:_____

Endereço: _____

CEP: _____Cidade: _____ UF: _____

Tel. Fixo 1: _____ Tel. Fixo 2: _____

Banco: _____ Agência: _____ c/c: _____

Dados do Representante Legal da Empresa:

Nome:_____

CPF/MF:_____Cargo/Função:_____

Cart.Ident nº:_____Expedido por: _____

Tel. Celular: _____ Tel. Celular 2: _____

Endereço eletrônico:_____

(Anexar comprovante de endereço)

Local e data.
Identificação e assinatura.

ANEXO V

ATA DE REGISTRO DE PREÇOS Nº ____/20____

Aos __ dias do mês de _____ do ano de 2.0____, o Instituto de Desenvolvimento do Trabalho - IDT, inscrito no CNPJ 02.533.538/0001-97 - Inscrição Estadual Isenta, com sede na Av. da Universidade n° 2596, Benfica, Fortaleza-CE por sua Diretoria em face do Pregão Eletrônico nº ___**/2.0**____, resolvem Registrar o(s) Preço(s) da empresa _____ _____, inscrita no CNPJ nº _____, Inscrição Estadual nº _____, com sede na _____ _____, CEP: _____, neste ato representada por seu representante legal _____, _____, _____, _____, portador do RG nº _____ expedido por ____/__ e no CPF/MF nº _____, observadas as condições constantes do Edital, da proposta da empresa e as indicados nesta Ata.

CLÁUSULA PRIMEIRA - FUNDAMENTO LEGAL

O presente instrumento fundamenta-se:

- No Pregão Eletrônico nº _____
- Na Lei Federal n.º 8.666, de 21.6.93 e suas alterações.

CLÁUSULA SEGUNDA - OBJETO

2.1. A presente Ata tem por objeto _____ _____ _____ cujas especificações e quantitativos encontram-se detalhados no Anexo I – Termo de Referência do edital de Pregão Eletrônico nº _____/20__ que passa a fazer parte desta Ata, juntamente com a(s) proposta(s) de preços apresentada(s) pelo(s) fornecedor(es) classificado(s) em primeiro lugar, conforme consta nos autos do Processo nº _____/_____.

2.1.1. Este instrumento não obriga a Administração a firmar contratações exclusivamente por seu intermédio, podendo realizar licitações específicas, obedecida a legislação pertinente, sem que, desse fato, caiba recurso ou indenização de qualquer espécie aos detentores do registro de preços, sendo-lhes assegurado a preferência em igualdade de condições.

CLÁUSULA TERCEIRA - DA VALIDADE

3.1. A presente Ata de Registro de Preços terá validade pelo prazo de 12(doze) meses contados a partir da data da sua assinatura.

CLÁUSULA QUARTA - DA UTILIZAÇÃO DA ATA DE REGISTRO DE PREÇOS

4.1. Em decorrência desta Ata, o participante do SRP poderá firmar contratos com os prestadores de serviços, com preços registrados, devendo comunicar ao órgão gestor, a recusa do detentor de registro de preços em executar o serviço no prazo estabelecido pelas Coordenação participantes.

4.1.1. O prestador do serviço terá o prazo de 5 (cinco) dias úteis, contados a partir da convocação, para a assinatura do contrato. Este prazo poderá ser prorrogado uma vez por igual período, desde que solicitado durante o seu transcurso e, ainda assim, se devidamente justificado e aceito.

4.1.2. Na assinatura do contrato será exigida a comprovação das condições de habilitação exigidas no edital, as quais deverão ser mantidas pela contratada durante todo o período da contratação.

CLÁUSULA QUINTA - DAS OBRIGAÇÕES

5.1. O detentor do registro de preços, durante o prazo de validade desta Ata, fica obrigado a:

5.1.1. Atender os pedidos efetuados pela(s) Coordenação(ões) participante(s) do SRP, bem como aqueles decorrentes de remanejamento registrados nesta Ata, durante a sua vigência.

5.1.2. Executar os serviços ofertados, por preço unitário registrado, nas quantidades e especificações indicadas no Edital e Termo de Referência – Anexo I**.**

CLÁUSULA SEXTA – DOS PREÇOS REGISTRADOS

6.1. Os preços registrados são os preços unitários ofertados nas propostas das signatárias desta Ata, anexas a este instrumento e servirão de base para futuras aquisições, observadas as condições de mercado.

CLÁUSULA SÉTIMA – DA REVISÃO DOS PREÇOS REGISTRADOS

7.1. O(s) preço(s) registrado(s) é(são) fixo(s) e irreajustável(is) durante a vigência da Ata de Registro de Preços, sendo entretanto, admitido o reequilíbrio econômico/financeiro, na hipótese de alterações do preço registrado em relação aos valores praticados no mercado, seja em decorrência da elevação ou redução, conforme previsto no item 17.6 e subitens, do Edital.

CLÁUSULA OITAVA – DO CANCELAMENTO DO REGISTRO DE PREÇOS

8.1 O fornecedor terá seu registro cancelado quando:

8.1.1. Deixar de cumprir as condições da Ata de Registro de Preços;

8.1.2. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior àqueles praticados no mercado;

8.1.3. Quando, justificadamente, não for mais do interesse do IDT.

8.2 O cancelamento do registro, na hipótese prevista no subitem 8.1, assegurados o contraditório e a ampla defesa, será precedido de autorização escrita e fundamentada da autoridade competente.

8.3 O fornecedor poderá solicitar o cancelamento do seu registro de preço na ocorrência de fato superveniente que venha comprometer a perfeita execução contratual decorrente de caso fortuito ou força maior, devidamente comprovado.

CLÁUSULA NONA - DAS CONDIÇÕES PARA A EXECUÇÃO

09.1. Os serviços que poderão advir desta Ata de Registro de Preços serão formalizadas por meio de instrumento contratual a ser celebrado entre o órgão participante/interessado e o prestador de serviço.

09.1.1. Caso o prestador de serviço classificado em primeiro lugar, não cumpra o prazo ou os pré-requisitos estabelecidos pelo IDT em Edital, ou se recuse a executar o serviço em conformidade com as regras do Pregão a que se acha subordinado, terá o seu registro de preço cancelado, sem prejuízo das demais sanções previstas em lei e no instrumento contratual.

09.1.2 - Neste caso, será convocado sucessivamente por ordem de classificação, os demais prestadores de serviços.

CLÁUSULA DÉCIMA - DO PAGAMENTO

10.1. As despesas decorrentes da Ata de Registro de Preços correrão pelas fontes de recursos das dotações orçamentárias do IDT, a ser informada quando da lavratura do instrumento contratual.

10.2 O(s) pagamento(s) será(ao) efetuado(s) até 10(dez) dias contados da data da apresentação da nota fiscal/fatura devidamente atestada pelo gestor da contratação.

10.2.1. A nota fiscal/fatura que apresente incorreções será devolvida à contratada para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

10.2.2. Não será efetuado qualquer pagamento à contratada, em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

10.2.3. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações do Anexo I – Termo de Referência do edital do Pregão Eletrônico nº ___/_____.

10.3. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em cartório. Caso esta documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

CLÁUSULA DÉCIMA PRIMEIRA - DAS SANÇÕES ADMINISTRATIVAS

11.1. O licitante que praticar quaisquer das condutas previstas no art. 32, do Decreto Estadual nº 28.089/2006, sem prejuízo das sanções legais nas esferas civil e criminal, estará sujeito às seguintes penalidades:

11.1.1. Multa de 10% (dez por cento) sobre o valor da proposta.

11.1.2. Impedimento de licitar e contratar com o Instituto de Desenvolvimento do Trabalho - IDT, sendo, então, descredenciado no cadastro de fornecedores, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste edital e das demais cominações legais.

11.2. O licitante recolherá a multa por meio de pagamento na Tesouraria do IDT podendo ser substituído por outro instrumento legal, em nome do órgão Contratante. Se não o fizer, será cobrada em processo de execução.

11.2.1. As multas porventura aplicadas poderão ser descontadas dos pagamentos devidos pela Contratante ou cobradas diretamente da Contratada, administrativa ou judicialmente, e podendo ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

11.2.2. O atraso injustificado no prazo de fornecimento implicará multa correspondente a 3,33% (três vírgula trinta e três por cento) por dia, calculada sobre o valor total do contrato ou da parcela dos serviços não cumprida, até o limite de **10%** (dez por cento) desse valor.

11.2.3. Na hipótese mencionada no item anterior, o atraso injustificado por período **superior a 05(cinco) dias** caracterizará o descumprimento total da obrigação, punível com a rescisão unilateral do contrato e suas conseqüências, e da aplicação da sanção prevista no item 11.1.2.

11.2.4. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério da Contratante.

11.3. Sempre que não houver prejuízo para a Contratante, as penalidades impostas poderão ser relevadas ou transformadas em outras de menor sanção, a seu critério.

11.4. As aplicações das penalidades serão precedidas de concessões de oportunidades de ampla defesa por parte da Contratada, na forma da lei.

CLÁUSULA DÉCIMA SEGUNDA - DO FORO

12.1. Fica eleito o foro do município da capital do Estado do Ceará, para conhecer das questões relacionadas com a presente Ata que não possam ser resolvidas pelos meios administrativos.

12.2. Assinam esta Ata, os signatários relacionados e qualificados a seguir, os quais firmam o compromisso de zelar pelo fiel cumprimento das suas cláusulas e condições.

Fortaleza, _____ de _____ 20____.

_____

Antônio Gilvan Mendes de Oliveira
Presidente do IDT

_____

Representante Legal da Empresa

TESTEMUNHAS:

Nome_____ Nome_____
CPF:_____ CPF:_____
RG:_____ RG:_____

ANEXO VI

MINUTA DE CONTRATO Nº _____ / 20__

CONTRATO QUE ENTRE SI FAZEM, DE UM LADO O INSTITUTO DE DESENVOLVIMENTO DO TRABALHO – IDT, E, DO OUTRO, A EMPRESA ....., PARA O FIM QUE NELE SE DECLARA

O INSTITUTO DE DESENVOLVIMENTO DO TRABALHO - IDT, inscrito no CNPJ/MF sob o nº 02.533.538/0001-97, sito na Avenida da Universidade, 2596 - Benfica, CEP 60.020-180, Fortaleza / CE, neste ato representado por seu Presidente, Antônio Gilvan Mendes de Oliveira, portador do CPF nº ....., doravante denominado simplesmente CONTRATANTE**,** e, de outro, a empresa ....., inscrita no CNPJ sob. nº ....., Inscrição Estadual ....., com sede na ...., neste ato representada por seu representante legal ...., (cargo na empresa) ....., portador da cédula de identidade RG nº ..... expedida pelo(a) ..... e inscrito no CPF/MF sob nº ....., doravante denominado CONTRATADA, firmam o presente Contrato, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO LEGAL

1.1. O presente contrato tem como fundamento o edital do Pregão Eletrônico n°_____/20____, e seus anexos, Ata de Registro nº _____/20_____,realizado de acordo com as normas da Lei N º. 10.520, de 17/07/2002, da Lei Federal nº 8.666/1993, com suas alterações, dos preceitos de direito aplicáveis, e, ainda supletivamente, nos princípios da teoria geral dos contratos e nas disposições do direito privado.

CLÁUSULA SEGUNDA – DA VINCULAÇÃO AO EDITAL E A PROPOSTA

2.1. O cumprimento deste contrato está vinculado aos termos do edital do Pregão Eletrônico nº _____/20___ e seus anexos, e à proposta da CONTRATADA, os quais constituem parte deste instrumento, independente de sua transcrição.

CLÁUSULA TERCEIRA – DO OBJETO

3.1. O presente Contrato tem por objeto _____, visando suprir as necessidades operacionais e administrativas do Instituto de Desenvolvimento do Trabalho – IDT.

CLÁUSULA QUARTA – DO VALOR

4.1. O valor global importa na quantia de R$ _____ (_____), sujeito a reajustes, desde que observado o interregno mínimo de 01 (um) ano, a contar da apresentação da proposta, mediante negociações entre as partes, tendo como limite máximo a variação do IGP/DI – FGV.

CLÁUSULA QUINTA – DOS RECURSOS ORÇAMENTÁRIOS

5.1. Os recursos necessários para a contratação do objeto para atender ao _____, conforme previsto no Contrato de Gestão Nº ___/20___

Item	Descrição

CLÁUSULA SEXTA – DOS PAGAMENTOS

6.1. O pagamento será efetuado até 10 (dez) dias contados da data da apresentação da Nota Fiscal e Recibo, devidamente atestada pelo gestor da contratação, acompanhada da Autorização de Serviço e da Documentação relativa à regularidade para com a Seguridade Social (INSS), Fundo de Garantia por Tempo de Serviço (FGTS),Trabalhista e Fazendas Federal, Estadual e Municipal, mediante emissão de cheque nominal ou depósito em conta bancária.

6.2. A nota fiscal/fatura que apresente incorreções será devolvida à CONTRATADA para as devidas correções. Nesse caso, o prazo de que trata o subitem anterior começará a fluir a partir da data de apresentação da nota fiscal/fatura corrigida.

6.3. Não será efetuado qualquer pagamento à CONTRATADA**,** em caso de descumprimento das condições de habilitação e qualificação exigidas na licitação.

6.4. É vedada a realização de pagamento antes da execução do objeto ou se o mesmo não estiver de acordo com as especificações deste instrumento.

6.5. Caso ocorra, a qualquer tempo, a não aceitação de qualquer parte do fornecimento, o prazo de pagamento será interrompido e reiniciado após a correção pela CONTRATADA.

6.6. Toda a documentação exigida deverá ser apresentada em original ou por qualquer processo de reprografia, obrigatoriamente autenticada em Cartório. Caso a documentação tenha sido emitida pela Internet, só será aceita após a confirmação de sua autenticidade.

CLÁUSULA SÉTIMA – DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO

7.1. O prazo de vigência deste contrato é de ___ (_____) meses, contado a partir da sua assinatura, devendo ser publicado na forma do parágrafo único, do art. 61, da Lei Federal nº 8.666/1993.

7.2. O prazo de execução do objeto deste contrato deverá obedecer, as especificações e as condições estabelecidas no Edital do Pregão Eletrônico Nº ___/20___ e seus anexos.

7.3. Os prazos de vigência e de execução deste contrato poderão ser prorrogados nos termos do que dispõe o art. 57, § 1º da Lei Federal n° 8.666/1993.

CLÁUSULA OITAVA – DA GARANTIA CONTRATUAL

8.1. Não será exigida prestação de garantia para esta contratação.

CLÁUSULA NONA – DO RECEBIMENTO

9.1. Em conformidade com os artigos 73 a 76 da Lei Nº 8.666/93, mediante recibo, os fornecimentos objeto deste contrato serão considerados recebidos depois que os prepostos dos beneficiários do contrato atestarem a conformidade do fornecimento com as faturas emitidas pela CONTRATADA.

9.2. Todo produto entregue em desacordo com as especificações será obrigatoriamente substituído em prazo satisfatório para devida realização do fornecimento do objeto do presente contrato, sem ônus para a CONTRATANTE.

9.3. Em conformidade com os artigos 73 a 76 da Lei Nº 8.666/93, mediante recibo, os fornecimentos objeto deste contrato serão considerados recebidos depois que os prepostos dos beneficiários do contrato atestarem a conformidade do fornecimento com as faturas emitidas pela CONTRATADA.

9.3.1. Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 02 (dois) dias úteis antes do término do prazo de execução, e aceitos pela contratante, não serão considerados como inadimplemento contratual.

9.4. O objeto contratual que comprovadamente apresentar desconformidade com as especificações do Termo de Referência será rejeitado, parcialmente ou totalmente, conforme o caso, obrigando-se o vencedor a substituí-los no prazo máximo de 48 (quarenta e oito) horas, sem ônus para a CONTRATANTE, sob pena de ser considerada em atraso quanto ao prazo da entrega.

CLÁUSULA DÉCIMA - DAS EXIGÊNCIAS DA CONTRATAÇÃO

10.1. A contratada irá responsabilizar-se, em caráter exclusivo, pela prestação dos serviços.

CLÁUSULA DÉCIMA PRIMEIRA– DAS OBRIGAÇÕES DA CONTRATADA

11.1. Fornecer o objeto da licitação, de acordo com as especificações definidas no Termo de Referência. Eventuais alterações deverão ser submetidas à apreciação e aprovação prévia do IDT, devendo estar garantidas, no mínimo, as especificações e certificações exigidas na licitação.

11.2. Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.

11.3. Atender a todas as obrigações de natureza fiscal que incidam ou venham a incidir sobre os fornecimentos e distribuições contratados.

11.4. Assumir plena e irrestrita responsabilidade por qualquer acidente ou incidente ocorrido, isentando totalmente o IDT de todas e quaisquer reclamações e indenizações que possam surgir em decorrência dos mesmos.

11.5. Instruir seu (s) empregado (s) e/ou prepostos, para que, ao entrar (em) nas dependências do IDT, apresente(m) sua identificação ao responsável pela portaria (recepção), para fim de registro.

11.6. Notificar o IDT, por escrito, caso ocorra qualquer fato que impossibilite o cumprimento das cláusulas contratuais dentro dos prazos previstos.

11.7. Aceitar, nas mesmas condições ora pactuadas, os acréscimos ou supressões que se fizerem necessários no percentual de até 25% (vinte e cinco por cento), do valor inicial atualizado.

11.8. Indicar, na hipótese de empresa domiciliada fora de Fortaleza, representante com poder de decisão, que tenha estabelecimento no município de Fortaleza e/ou Região Metropolitana, para representá-lo durante a execução do contrato.

11.9. Assumir integral responsabilidade pela inexecução parcial ou integral dos serviços prestados, bem como pelos atos omissivos ou comissivos praticados pelos seus empregados, sujeitando às condições e penalidades previstas.

11.10. Responsabilizar-se por todo e qualquer espécie de dano causado por seus empregados em face dos serviços, bem como pelo extravio de coisas ocorridas na prestação dos serviços.

11.11. Adotar gestões tempestivas, diligentes e imediatas no sentido de corrigir as eventuais falhas ou problemas apurados na execução dos serviços.

11.12. Relatar à contratante as ocorrências contratuais.

11.13. Assegurar-se que o local de instalação dos equipamentos necessários à Prestação dos Serviços neste edital precificada possui as condições técnicas e ambientas necessárias ao pleno, seguro e normal funcionamento dos equipamentos necessários à prestação dos serviços.

11.14. Especificar e requerer do SINE-IDT/CE as condições técnicas e ambientais para a instalação das Soluções em no máximo 48 (quarenta e oito) horas úteis do recebimento da Solicitação de Serviço para implantação das soluções e serviços contratados.

11.15. Manter os Centros de Operação de Segurança e Rede (SNOC) próprios para monitoramento remoto 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), com infra-estrutura estritamente de acordo com as especificações deste documento.

11.16. Implantar todos os softwares e hardwares necessários à prestação dos serviços de monitoração, gerência e administração remota da segurança, conforme todas as especificações técnicas constantes no Edital do Pregão Nº 05/2016 e seus anexos.

11.17. Responsabilizar-se pela manutenção preventiva e corretiva dos hardwares e softwares por ela ofertados.

11.17.1. **Todas as soluções de hardwares e softwares, ambientes de gerenciamento e monitoramento devem ser fornecidos em regime de locação.**

11.18. Iniciar a Prestação dos Serviços rigorosamente em estrita observância aos prazos estabelecidos no Edital e seus anexos.

11.19. Implementar/gerenciar o backup de configuração de sistemas (regras) e análise de logs.

11.20. Realizar qualquer alteração na configuração da solução (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de "patches" e correlatos.) mediante autorização formal do SINE-IDT/CE.

11.21. Comunicar, imediatamente, a eminência ou ocorrência de 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 SINE-IDT/CE.

11.22. Responsabilizar-se inteiramente por todas as implantações das soluções.

11.23. Resolver os chamados de Serviço e Suporte Técnico conforme os tempos definidos nas tabelas de tempos de atendimento (SLA) deste Termo de Referência.

11.23.1. A substituição de Equipamentos com Defeito, que cause a Indisponibilidade de Serviço fica direta e estritamente vinculada em conformidade com o tempo estipulado na Tabela de Tempos de Atendimento (SLA).

11.24. Manter os serviços contratados em cumprimento aos Níveis de Disponibilidade estabelecidos no item 06 do Termo de Referência – anexo I do Edital.

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

11.25. Responsabilizar-se por efetuar as atividades de integração da solução de monitoração remota com o ambiente operacional do SINE-IDT/CE, sem prejuízo aos serviços desta.

11.26. 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 SLA estabelecido no Edital e seus anexos.

11.27. Produzir e enviar por e-mail, mensalmente, relatórios analíticos a equipe gestora do SINE-IDT/CE, ou em 24 (vinte e quatro) horas quando houver demanda.

11.28. **Participar, mensalmente, de reuniões presenciais**, de ponto de controle, para apresentação dos indicadores de disponibilidade, diagnósticos dos ambientes monitorados, dirimir dúvidas sobre os serviços contratados, análise e entendimento dos relatórios gerenciais e administrativos, revisão das configurações e procedimentos implementados e melhorias a serem implementadas.

11.29. 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 SINE-IDT/CE, praticado por seus empregados, conforme **TERMO DE CONFIDENCIALIDADE**, anexo a este Contrato.

CLÁUSULA DÉCIMA SEGUNDA – DAS OBRIGAÇÕES DA CONTRATANTE

12.1. Emitir as autorizações de execução de serviços, numeradas, assinadas pela autoridade competente.

12.2. Proporcionar à CONTRATADA todas as facilidades indispensáveis ao bom cumprimento da execução do objeto contratual.

12.3. Notificar a CONTRATADA relativamente a qualquer irregularidade encontrada na execução dos serviços.

12.4. Emitir atestados de capacidade técnica quando solicitados.

12.5. Zelar pela pontualidade dos pagamentos decorrentes da execução do contrato, inclusive, aqueles devidos pelos beneficiários.

12.6. Solicitar a execução do objeto à CONTRATADA através da emissão de Autorização de Serviço.

12.7. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

12.8. Assegurar-se da correta cobrança dos serviços, observadas as glosas, antes de cada pagamento, bem como a apresentação dos documentos comprobatórios necessários.

12.9. Não permitir que outrem execute o objeto Contratado.

12.10. Efetuar, quando julgar necessário, inspeção com a finalidade de verificar a prestação dos serviços e o atendimento das exigências contratuais.

12.11. Comunicar à CONTRATADA toda e qualquer ocorrência relacionada com a execução do serviço.

12.12. Efetuar o pagamento à CONTRATADA pelos serviços prestados, nas condições e preços pactuados, à vista da Nota Fiscal/Fatura, devidamente atestada, depois de constatado o cumprimento de todas as formalidades e exigências contratuais.

12.13. Aplicar penalidades e multas à CONTRATADA, mediante o devido processo legal, garantido a ampla defesa e o contraditório.

12.14. Exigir, mensalmente, os documentos comprobatórios para o pagamento, conforme especificado na cláusula sexta.

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

12.16. 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 que se tornem necessárias.

12.17. Informar aos técnicos da Contratada as necessidades de configuração dos equipamentos e serviços, por meio da abertura de chamados de suporte técnico, e quando necessário, podem ser anexados aos chamados arquivos com as necessidades de configurações.

12.18. Cumprir pontualmente todos os seus compromissos financeiros para com a Contratada.

12.19. Proporcionar todas as facilidades para que a Contratada possa executar os serviços dentro das normas e condições estabelecidas neste Contrato.

12.20. Comunicar à Contratada todas as possíveis irregularidades detectadas na execução dos serviços contratados.

12.21. Fiscalizar e acompanhar a execução dos serviços.

12.21.1. Atestar a sua prestação se, e somente se, os serviços executados atenderem plenamente às especificações constantes no Edital.

12.21.2. Rejeitar, no todo ou em parte, a solução entregue pela Contratada fora das especificações do Edital.

12.21.3. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada pelos danos causados ao SINE-IDT/CE ou a Terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos.

CLÁUSULA DÉCIMA TERCEIRA – DA DESCRIÇÃO DO SERVIÇO (METODOLOGIA)

13.1. A Licitante Vencedora deverá cumprir com todos os requisitos especificados no todo deste edital, e sem nenhuma exceção, sob pena de desclassificação imediata e atendendo a tudo quanto também estará abaixo elencado, no que se refere aos serviços a serem prestados e ora objeto deste edital:

13.2. Implantação das Soluções

13.2.2. A Contratada deverá realizar a prestação dos serviços e implantação das soluções, mediante solicitação e com configuração, instalação, testes e fornecimentos dos hardwares e softwares relacionados, em regime de locação, para todas as soluções e serviços contratados através de utilização obrigatória de SNOC e profissionais capacitados e certificados pelos fabricantes.

13.2.3.Todas as atividades envolvidas e decorrentes da prestação dos serviços e implantação das soluções serão devidamente acompanhadas e coordenadas por analistas e técnicos do SINE - IDT/CE.

13.2.4. A implantação das soluções, quando realizadas no ambiente de produção, poderá exigir a necessidade de que as atividades sejam realizadas após o expediente (horários noturnos e/ou em finais de semana e feriados) a fim de não comprometer o normal funcionamento das atividades do SINE - IDT/CE.

13.2.5. A Contratada será responsável por efetuar as atividades de integração de todas as soluções aqui previstas, especialmente quanto aquelas de monitoração remota, de service desk, correlação de eventos e todas as demais no ambiente operacional do SINE - IDT/CE, sem prejuízo aos serviços deste e nas localidades e onde o SINE - IDT/CE solicitar.

13.3. Prestação dos Serviços Contínuos

13.3.1. Os serviços poderão ser prestados remotamente, não estando excluída a prestação de serviços in loco (significando dizer, na língua pátria: no local) de técnicos capacitados e certificados da Contratada e diante de solicitações que venham a ocorrer.

13.3.1.1 O suporte técnico e atendimento remoto serão executados obrigatoriamente a partir de 2 (dois) Centros de Operação de Segurança e Redes (SNOC) redundantes da Contratada, sendo o primeiro localizado em Fortaleza/Ce e o segundo necessariamente em outro estado da Federação, para permitir plena operacionalidade em vista de eventual ocorrência de parada de um deles.

13.3.1.2 Os referidos Centros de Operação serão objeto de comprovação documental conforme item 5 deste Termo, e se necessário também, através de diligências que serão efetuadas por técnicos do SINE-IDT/CE, sendo igualmente exigida a comprovação da existência de todos os requisitos especificados neste documento, inclusive, a obrigatoriedade de já estar em pleno funcionamento na data da publicação do edital.

13.3.2. Os serviços de monitoração remota das soluções e serviços aqui contemplados deverão ser realizados pela Contratada, na modalidade 24x7x365 (vinte e quatro horas por dia, sete dias na semana, todos os dias do ano). Há previsibilidade de interação presencial no caso de necessidades que possam vir a ocorrer e sem limite para tanto.

13.3.3. Para a manutenção dos hardwares e softwares ofertados, bem como para a prestação do suporte técnico aos serviços de monitoração remota, a Contratada deverá já possuir infra-estrutura de suporte técnico, disponível em período integral, ou seja, 24x7x365 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano), nos seguintes modelos:

13.3.3.1. Suporte técnico remoto: suporte prestado por meio de Central de Atendimento 0800 ou equivalente à ligação local para:

13.3.3.2. Esclarecimento de dúvidas relacionadas à prestação dos serviços, políticas e regras implementadas, funcionalidade das soluções e incidentes de segurança, sendo este atendimento imediato.

13.3.3.3. Atendimento às solicitações de alterações (inclusão e exclusão) de políticas e regras. Atendimento às solicitações de log e relatórios.

13.3.3.3.1. Suporte técnico local: atendimento in loco, prestados por técnicos capacitados e certificados em quantidade suficiente para prestar todos os serviços conforme estabelecido no contexto geral deste edital, para a solução de eventuais problemas relacionados aos serviços, equipamentos, soluções e softwares ofertados.

13.3.4. As versões dos softwares ofertados pela Contratada sempre deverão estar com a versão mais atual disponível no mercado. A versão anterior:

13.3.4.1. Não poderá permanecer instalada mais do que 3 (três) meses, após o lançamento da última versão homologada; ou

13.3.4.2. Poderá permanecer instalada por tempo maior, desde que acordado com o SINE-IDT/CE.

13.3.5. A Contratada deverá disponibilizar sem ônus adicional, para utilização nas instalações do SINE - IDT/CE, de até 4 (quatro) telas de LCD de 40” para permitir a visualização e o acesso de

leitura a console de gerenciamento e monitoramento de todas as soluções ofertadas cujas implementações também serão de responsabilidade única da Contratada.

13.3.6. Serão apresentados pela Contratada, no mínimo, relatórios analíticos mensais contendo o diagnóstico dos ambientes monitorados, obtido através do cruzamento das informações coletadas pelos softwares destinados a esse fim e de responsabilidade exclusiva da Contratada. Tais relatórios deverão estar disponíveis para o SINE - IDT/CE a qualquer momento, se solicitado, devendo ser disponibilizados em até 24 (vinte e quatro) horas após a solicitação.

13.3.7. Os recursos humanos envolvidos nas atividades de monitoração remota da segurança deverão ser suficientes e dedicados às atividades de monitoração e de pleno conhecimento e reconhecimento por parte do SINE-IDT/CE, ou seja, estando sempre disponíveis para executar as atividades exigidas no contexto geral deste edital, mormente porque ocorrerá certamente atendimentos presenciais.

13.3.8. Os recursos humanos envolvidos na prestação de serviço de monitoração e suporte técnico das soluções e serviços contratados deverão conhecer e estar capacitados e certificados em todas as soluções contempladas neste edital. Entende-se por capacitação: **certificados e/ou atestados profissionais emitidos pelos fabricantes e/ou distribuidores oficiais dos fabricantes ou instituições independentes que deverão ser apresentados na proposta.**

13.3.9. A Contratada deverá interagir com os analistas e técnicos do SINE-IDT/CE para dirimir/explicitar/equacionar dúvidas/questionamentos relacionadas aos serviços prestados, mediante atendimento telefônico por central 0800 ou equivalente à ligação local, assim como na forma presencial quando solicitada.

13.3.10. A Contratada deverá disponibilizar também um sistema de abertura de chamados via WEB com aderência as melhores práticas ITIL conforme descrito no item 13.3.10.1. e seguintes. A Licitante deverá informar todo processo de abertura de chamados. Esta comprovação deverá ser realizada já na fase de apresentação dos documentos de habilitação e não ocorrência da referida comprovação será motivo suficiente para a desclassificação da mesma, ato contínuo.

13.3.10.1. A ferramenta a ser utilizada para gestão de todo o processo de atendimento de chamados (Service Desk) deverá no mínimo, conter/apresentar as funcionalidades mínimas conforme abaixo descritas:

13.3.10.1.1. A plataforma deve comprovar aderência, no mínimo ao **ITIL 2011** através da apresentação da certificação PinkVerify para os processos de Gerenciamento de Incidentes, Requisições e Catálogo de Serviços.

13.3.10.1.2. Deve possuir estrutura de desenvolvimento, manutenção e suporte da ferramenta no Brasil.

13.3.10.1.3. O software deve possuir documentação online para permitir acesso a consultas, também sendo capaz de orientar seus usuários e contendo às informações de conteúdo no idioma Português/Brasil.

13.3.10.1.4. Suportar a abertura de chamados mediante a utilização de aplicação nativa para dispositivos móveis baseados em Android e IOS.

13.3.10.1.5. Possibilitar utilização de relatórios e estatísticas através da definição de filtros de pesquisa diretamente na interface do software e sem necessidade de software adicional.

13.3.10.1.6. Possibilitar a impressão de relatórios, estatísticas e resultados de pesquisas.

13.3.10.1.7. Garantir a definição de controles de níveis de acesso aos dados quando da elaboração/confecção dos relatórios.

13.3.10.1.8. Permitir a inclusão de logotipo da Contratante em telas e relatórios, com base em parametrização.

13.3.10.1.9. Permitir a exibição de indicadores em formato de gráficos com as respectivas definições de faixas de valores de forma configurável.

13.3.10.1.10. Possuir recursos para constituição de uma base de conhecimentos técnicos, operacionais, normativos e administrativos.

13.3.10.1.11. Possibilitar o fornecimento para cada registro um número único, registrando também a data e hora de abertura e data e hora da última atualização dos registros de incidentes e requisições de serviços.

13.3.10.1.12. Possibilitar ao atendente que estiver fazendo uso da interface do Software, classificar o impacto e a urgência de sua solicitação de acordo com uma pré-configuração.

13.3.10.1.13. Permitir que a classificação/ categorização possa ser alterada, a qualquer tempo e por quem for autorizado, mantendo, porém, o registro das alterações para consultas futuras.

13.3.10.1.14. Possibilitar a definição automática de prioridade do chamado de acordo com o nível de interrupção de serviço informado.

13.3.10.1.15. Possibilitar a definição de tempos de atendimento (SLA's) contendo os parâmetros de prazos de respostas e resolução dos incidentes/requisições, conforme a severidade associada e precificada neste edital.

13.3.10.2. Os chamados abertos só poderão ser fechados após autorização de funcionário designado pelo SINE-IDT/CE e deverão aguardar um prazo mínimo de 2 (dois) dias para a aprovação por parte da Contratante.

13.3.10.3. O SINE-IDT/CE informará as pessoas autorizadas a abrir e fechar chamados junto à Contratada.

13.3.10.4. A Contratada será responsável, sem ônus adicional ao SINE-IDT/CE por ministrar **treinamento para até 7 (sete) pessoas pertencentes ao quadro funcional do IDT** para as Soluções de Firewall, através de Instrutor Oficial do Fabricante, ficando facultado, a critério exclusivo do SINE-IDT/CE a solicitação para aplicação do exame oficial para certificação em Centro de Certificação Oficial, também sem qualquer ônus adicional.

13.3.11. Manutenção das Regras e Políticas e versões dos Softwares

13.3.11.1. Toda e qualquer alteração na configuração das soluções (aplicação de novas regras, exclusão de regras, atualização de versões, aplicações de "patches", entre outras correlatas) deverá ocorrer mediante autorização do SINE-IDT/CE.

13.3.11.2. O SINE-IDT/CE, no momento da implantação das soluções, indicará as pessoas que poderão autorizar as referidas alterações.

13.3.12. As alterações das configurações deverão ocorrer em horários determinados pelo SINE-IDT/CE.

13.3.13. O tempo de atendimento às solicitações de alterações das políticas e regras feitas pelo SINE-IDT/CE não deverá ultrapassar o SLA (Acordo de Nível de Serviço) especificado neste documento, a contar da efetivação das solicitações.

13.3.14. A Contratada deverá efetuar, em laboratório próprio, os testes necessários antes de implementação de qualquer alteração no ambiente de monitoração (políticas, regras, versões e correlatos), evitando impactos negativos nos serviços do SINE-IDT/CE salvo se, pela urgência este último dispensar os testes preliminares.

13.3.14.1. Caso sejam solicitadas alterações substanciais na configuração e forma de aplicação das tecnologias especificadas no edital, o SLA para tais solicitações poderá ser prorrogado a fim de permitir a devida execução de testes e validação das configurações visando garantir a correta implementação para o bom e regular funcionamento das soluções.

13.3.14.2. O SINE-IDT/CE poderá solicitar a qualquer tempo e por escrito, o acesso às senhas de configuração dos equipamentos disponibilizados pela Contratada em regime de locação. O SINE-IDT/CE designará duas pessoas para terem acesso às senhas, que devem ser fornecidas de forma segura. O SINE-IDT/CE deverá seguir os procedimentos documentais acordados entre as partes, caso venha a fazer uso deste acesso, e se responsabilizará pelas consequências que porventura possam advir diante da possibilidade de ocorrência de acessos.

13.3.15. Controle dos Serviços Realizados pela CONTRATADA

13.3.15.1. Para o controle e administração dos serviços realizados pela Contratada, o SINE-IDT/CE poderá nomear até 3 (três) representantes autorizados a interagir com aquela. Tais representantes serão responsáveis por:

13.3.15.1.1. Manter as informações técnicas (configuração do ambiente) atualizadas, bem como dar suporte na implantação e manutenção das soluções a serem utilizadas.

13.3.15.1.2. Definir as estratégias, políticas e regras a serem implantadas, além de analisar os relatórios gerados pelos softwares que compõem as soluções ofertadas.

13.3.15.1.3. Tomar todas as providências necessárias em caso da ocorrência de algum incidente (análise dos logs, rastreamento da ocorrência, por exemplo).

13.3.15. Para cada solução implantada a Contratada emitirá relatórios definidos pelo SINE-IDT/CE, mas em conformidade com as informações nele disponibilizadas pelo fabricante, este o responsável pela fabricação do software a ser utilizado.

13.3.15.1. A Contratada poderá, caso seja solicitado, realizar reuniões mensais, nas dependências do SINE-IDT/CE para dirimir quaisquer dúvidas sobre os serviços contratados, análise e entendimento dos relatórios gerenciais e administrativos e revisão das configurações e procedimentos implementados. Para tanto, agendará as datas das reuniões com antecedência mínima de 5 (cinco) dias corridos da data desejada mais próxima.

13.3.15.2. O SINE-IDT/CE poderá, a qualquer tempo realizar auditoria nas instalações dos Centros de Operações de Segurança e Rede (SNOC), com o objetivo de verificar as instalações físicas, a segurança física e lógica do ambiente, e demais itens exigidos neste documento, desde que previamente acordada com a Contratada.

13.3.16. Ocorrência de Incidentes

13.3.16.1. No caso de detecção de algum incidente de segurança, a Contratada pode acionar o SINE-IDT/CE imediatamente, para que sejam tomadas as medidas corretivas e legais necessárias, de acordo com o procedimento de resposta a incidentes aqui especificados.

13.3.16. Serão considerados incidentes de segurança, por exemplo: 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 SINE-IDT/CE.

13.3.16.1. A Contratada deverá comunicar imediatamente o SINE-IDT/CE, para que possa ser tomada ações preventivas, nos casos de tentativas de acessos indevidos, de instalação de códigos maliciosos, ou de qualquer outra ação que venha colocar em risco a segurança do ambiente do SINE-IDT/CE, mesmo que a ocorrência não tenha logrado êxito/ sem sucesso, mas que seja detectada a insistência por parte da pessoa mal intencionada.

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

13.3.16.1. Dependendo do grau do incidente, a Contratada deverá deslocar recursos técnicos capazes de dar suporte *in loco* objetivando, de imediato, resolução ao problema, para compor o tempo de resposta do SINE-IDT/CE, visando também dirimir quaisquer dúvidas e dar suporte nas providências a serem customizadas.

13.3.17. Soluções de Hardware e Software da CONTRATADA

13.3.17.1. Os Softwares e Hardwares necessários para implantação do serviço de monitoração, gerência e administração remota das soluções de segurança ofertadas fazem parte dos serviços a serem prestados pela Contratada durante o prazo de vigência do Contrato e sendo de sua exclusiva responsabilidade quanto a aquisição, manutenção, atualização vez que o modelo de contratação prevê a locação deles.

13.3.17.2. A manutenção das Licenças dos Hardwares e Softwares necessários, junto aos fabricantes, será de responsabilidade da Contratada, devendo esta apresentar cópia autenticada de aquisição das mesmas, anualmente ao SINE-IDT/CE.

13.3.17.3. Os Hardwares e Softwares ofertados deverão ser totalmente compatíveis com o ambiente operacional do SINE-IDT/CE, não sendo assim aceito, em nenhuma circunstância em caso de

incompatibilidade de qualquer ordem a fim de se manter a interoperabilidade de todos os recursos em utilização.

13.3.17.4. A Contratada é/ será sempre a única responsável por atividades que tenha como objetivo a manutenção preventiva e corretiva dos Hardwares por ela ofertados.

13.3.17.5. Tanto os Hardwares quanto os Softwares utilizados/ a serem utilizados devem ser fornecidos em regime de locação como já amplamente mencionado e entendido no contexto geral deste edital.

13.3.18. Encerramento dos Serviços de Monitoração Remota da Segurança

13.3.18.1. Quando do encerramento da prestação do serviço de monitoração remota da segurança, a Contratada deverá retirar os componentes da solução, comunicando a retirada ao SINE-IDT/CE, por escrito, com 30 (trinta) dias de antecedência.

13.3.18.2. Todas as informações de customização, políticas e regras, logs de auditoria serão disponibilizadas para o SINE-IDT/CE, em mídia magnética ou via rede, e em seguida eliminadas da base de dados da Contratada.

CLÁUSULA DÉCIMA QUARTA – DO ACOMPANHAMENTO E FISCALIZAÇÃO

14.1. A execução contratual será acompanhada e fiscalizada pelo(a) Sr(a). _____, _____, especialmente designado para este fim pela CONTRATANTE, de acordo com o estabelecido no art. 67, da Lei Federal nº 8.666/1993, doravante denominado simplesmente de GESTOR, a quem competirá, entre outras atribuições:

14.1.1. Solicitar à CONTRATADA e seus prepostos, ou obter do IDT, tempestivamente, todas as providências necessárias ao bom andamento da execução do objeto contratado e anexar aos autos do processo correspondente cópia dos documentos escritos que comprovem essas solicitações de providências.

14.1.2. Verificar a conformidade da execução do fornecimento com as normas especificadas no Termo de Referência do Edital.

14.1.3. Encaminhar à autoridade competente, fazendo juntada dos documentos necessários, relatório das ocorrências (falhas) observadas na execução do contrato, bem como as solicitações de penalidades aplicáveis pelo não cumprimento de obrigações assumidas pela CONTRATADA.

14.1.4. A ação do gestor do contrato não exonera a CONTRATADA de suas responsabilidades contratuais.

14.1.5 Ordenar à CONTRATADA troca ou substituição dos serviços e/ou produtos, no caso de defeito do objeto, imperfeições ou em desacordo com as especificações.

14.1.6. Atestar o recebimento do objeto contratual.

CLÁUSULA DÉCIMA QUINTA – DAS SANÇÕES

15.1. O licitante que praticar quaisquer das condutas previstas no art. 32, do Decreto Estadual nº 28.089/2006, sem prejuízo das sanções legais nas esferas civil e criminal, estará sujeito às seguintes penalidades:

15.1.1. Multa de 10% (dez por cento) sobre o valor da proposta.

15.1.2. Impedimento de licitar e contratar com o Instituto de Desenvolvimento do Trabalho - IDT, sendo, então, descredenciado no cadastro de fornecedores, pelo prazo de até 5 (cinco) anos, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, sem prejuízo das multas previstas neste edital e das demais cominações legais.

15.2. O licitante recolherá a multa por meio de pagamento na Tesouraria do IDT podendo ser substituído por outro instrumento legal, em nome do órgão Contratante. Se não o fizer, será cobrada em processo de execução.

15.2.1. As multas porventura aplicadas poderão ser descontadas dos pagamentos devidos pela Contratante ou cobradas diretamente da Contratada, administrativa ou judicialmente, e podendo ser aplicadas cumulativamente às demais sanções previstas nesta cláusula.

15.2.2. O atraso injustificado no prazo de fornecimento implicará multa correspondente a 3,33% (três vírgula trinta e três por cento) por dia, calculada sobre o valor total do contrato ou da parcela dos serviços não cumprida, até o limite de **10%** (dez por cento) desse valor.

15.2.3. Na hipótese mencionada no item anterior, o atraso injustificado por período **superior a 05(cinco) dias** caracterizará o descumprimento total da obrigação, punível com a rescisão unilateral do contrato e suas conseqüências, e da aplicação da sanção prevista no item 15.1.2.

15.2.4. Serão considerados injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério da Contratante.

15.3. Sempre que não houver prejuízo para a Contratante, as penalidades impostas poderão ser relevadas ou transformadas em outras de menor sanção, a seu critério.

15.4. As aplicações das penalidades serão precedidas de concessões de oportunidades de ampla defesa por parte da Contratada, na forma da lei.

CLÁUSULA DÉCIMA SEXTA – DA FRAUDE E DA CORRUPÇÃO

16.1. O CONTRATADO deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação, de contratação e de execução do objeto contratual. Para os propósitos desta clausula, definem-se as seguintes práticas:

a) **"prática corrupta"**: oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

b) **"prática fraudulenta":** a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

c) **"prática conluiada"**: esquematizar ou estabelecer um acordo entre dois ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não-competitivos;

d) **"prática coercitiva"**: causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando influenciar sua participação em um processo licitatório ou afetar a execução do contrato.

e) **"prática obstrutiva":**

(1) destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista nesta cláusula;

(2) atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

16.2. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

16.3. Considerando os propósitos dos itens acima, o contratado deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

16.4. O contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei nº 8.666, de 21 de junho de 1993, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

CLÁUSULA DÉCIMA SETIMA – DA RESCISÃO

17.1. Constituem motivos para rescindir o presente contrato, situações previstas nos artigos 77 a 80 da Lei 8.666/93 e suas alterações, sem que assista à CONTRATADA o direito de reclamar quaisquer indenizações relativas a despesas decorrentes de encargos provenientes da execução deste contrato.

17.2. O IDT, na condição de CONTRATANTE, se reserva o direito de considerar rescindido o presente contrato, em virtude do descumprimento de qualquer obrigação nele estabelecida, independentemente de interpelação judicial ou extrajudicial, sem que caiba a CONTRATADA qualquer indenização.

17.3. O CONTRATANTE poderá, também, unilateralmente, considerar rescindido o contrato, quando não houver mais interesse de continuar com o serviço por conveniência da administração, manifestando-se por escrito, com antecedência mínima de 30 (trinta) dias.

CLÁUSULA DÉCIMA OITAVA – DAS ALTERAÇÕES DO CONTRATO

18.1. Competem a ambas as partes, de comum acordo, salvo nas situações tratadas neste instrumento, na Lei Nº 8.666/93 e em outras disposições legais pertinentes, realizar, via termo aditivo, as alterações contratuais que julgarem convenientes.

18.2. O CONTRATADO, no curso da vigência contratual, se obriga a aceitar, nas mesmas condições ora pactuadas os acréscimos ou supressões que se fizerem necessários no percentual de até 25% (vinte e cinco por cento), do valor inicial atualizado.

CLÁUSULA DÉCIMA NONA– DA PUBLICAÇÃO

19.1. A publicação resumida do presente contrato no Diário Oficial, que é condição indispensável para sua eficácia, será providenciada pela CONTRATANTE, nos termos do parágrafo único do artigo 61 da Lei nº 8.666/93.

CLÁUSULA VIGÉSIMA – DAS CONDIÇÕES DE HABILITAÇÃO DA CONTRATADA

20.1. A CONTRATADA declara, no ato de celebração do presente contrato, estar plenamente habilitada à assunção dos encargos contratuais e assume o compromisso de manter, durante toda a execução do contrato, todas as condições de habilitação e qualificação exigidas na licitação.

CLÁUSULA VIGÉSIMA PRIMEIRA – DO FORO

21.1. As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas no foro da cidade de Fortaleza-CE.

E, por estarem de acordo com o ajustado, as partes assinam o presente instrumento, depois de lido e achado conforme perante as testemunhas que também assinam, em 03 (três) vias, de igual teor, para um só efeito jurídico.

Fortaleza, _____ de _____ 201__.

_____

Antônio Gilvan Mendes de Oliveira
Presidente do IDT

_____

Representante Legal da Empresa

TESTEMUNHAS:

Nome_____ Nome_____

CPF:_____ CPF:_____

RG:_____ RG:_____

ANEXO VII
TERMO DE CONFIDENCIALIDADE

_____doravante denominada **CONTRATADA**, estabelecida à _____, inscrita no CNPJ/MF sob n.º_____, neste ato devidamente representada por seu _____ (qualificação e nome).

Instituto de Desenvolvimento do Trabalho - IDT, doravante denominado **CONTRATANTE**, estabelecida à Av. da Universidade, 2596 – Benfica, na Cidade de Fortaleza - Estado do Ceará – CEP 60020-180, regularmente inscrita no CNPJ/MF sob o nº 02.533.538/0001-97, neste ato devidamente representada por seu(s) _____ (qualificação e nome).

A **CONTRATADA** compromete-se a manter sigilo a partir da data de assinatura deste termo, sobre todas as informações, técnicas e documentos que tomar conhecimento, excetuando-se aquelas que:

(i) ao tempo de sua transmissão à parte receptora, ou posteriormente, tais informações sejam ou venham a ser de domínio público, conforme evidenciado por publicações idôneas, desde que a divulgação não tenha sido causada pela própria parte receptora;

(ii) quando a informação se tornar pública por órgãos de proteção a propriedade industrial no Brasil ou Exterior;

(iii) ao tempo de sua transmissão à parte receptora, a informação já seja do conhecimento desta e não tenha sido obtida da parte reveladora, direta ou indiretamente, desde que esse fato seja comprovado por documento escrito;

(iv) as informações sejam obtidas de terceiros e sobre as quais nem as partes nem qualquer terceiro estejam igualmente obrigados a manter sigilo;

(v) no que diz respeito às informações que, por autorização escrita da parte proprietária, tiveram sido liberadas do seu status de confidencial.

Todas as informações confidenciais permanecerão de propriedade da **CONTRATANTE**.

Ao final do contrato, a parte receptora das informações deverá devolver prontamente à outra parte ou destruir com segurança todas as informações confidenciais recebidas, juntamente com cópias que estejam em seu poder.

As informações recebidas em sigilo não poderão ser utilizadas para fins próprios, com ou sem finalidade econômica.

No caso de infração deste **TERMO DE CONFIDENCIALIDADE** fica a **CONTRATADA** sujeita as penalidades civis e penais.

Estando ciente de tudo, a **CONTRATADA** assina a presente em 2 (duas) vias de igual teor e forma.

Fortaleza, ... de ..... de ..... .

_____
CONTRATADA

Testemunhas:

Nome:	**Nome:**
RG:	RG:
CPF:	CPF: