ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
TERMO DE REFERÊNCIA – TR

AQSETIN2018003 – Firewall de Nova Geração

1. OBJETO DA CONTRATAÇÃO

1.1. Constitui objeto deste Termo de Referência, Registro de preços para futura e eventual contratação de empresa especializada para o fornecimento de solução de segurança de perímetro com características de Next Generation Firewall, instalação, configuração, migração, garantia e suporte técnico pelo período de 60 (sessenta) meses.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Quantitativo

2.1.1. Fornecimento de appliances com características de Next Generation Firewall, compreendendo aquisição de equipamentos, conforme tabela abaixo e seus respectivos **ANEXOS I, II e III**:

BEM	ESTIMATIVA	FORMA DE ESTIMATIVA
Solução de Plataforma de Segurança em cluster, no mínimo: 02 (dois) Firewalls de Próxima, para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo Geração. Serviço de instalação e configuração devem estar incluídos.	1	Substituição da solução existente na segurança de Perímetro e inclusão de solução de segurança de Data Center.
Garantia da Solução de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em Português por autorizada credenciada e com serviço de suporte técnico remoto por 12 meses a ser prestado pela CONTRATADA.	60	
Software com licenciamento de uso perpétuo para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução em cluster. Com no mínimo, 60 meses de suporte.	1	
Módulo de Interface 1000BASE-T	2	

Módulo de interface 10GBASE-SR	14	
Software para Gerenciamento da Solução de Segurança em cluster.	1	
Garantia do Software para Gerenciamento da Solução de Segurança em cluster com Suporte Oficial do fabricante, através da Contratada, 24x7 fornecido no Brasil em Português. Com no mínimo, 60 meses de suporte.	60	

2.2. Motivação

O Poder Judiciário Cearense com o intuito de prover a segurança de rede e controlar os acessos à internet, protegendo contra possíveis tentativas de acesso indevido adquiriu através do contrato CT Nº 73/2010, celebrado com a empresa Lanlink Informática LTDA., uma solução de segurança de rede (Firewall) composta por:

- 03 (três) equipamentos concentradores de Firewall;
- 26 (vinte e seis) equipamento de VPN;
- 02 (dois) equipamentos de IPS;

Firewall é o nome dado ao dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede. Sua função consiste em regular, analisar e determinar quais operações de transmissão ou recepção de dados podem ser executadas a partir de um conjunto de regras ou instruções.

A sua finalidade consiste em bloquear o tráfego de dados indesejado e liberar acessos impedindo a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra.

A infraestrutura mencionada é utilizada pelo Judiciário Cearense sendo formada por equipamentos e softwares de gerência, que compõem a solução de perímetro de segurança da informação que provê, além da segurança, a integridade dos dados trafegados entre os serviços Judiciais – SAJPG, SAJSG, SPROC e PROJUDI/PJE e Administrativos – CPA, SGF, ALX, GRH,

SCL, SMO, SCO, SGV, PEX, SIP e SPD através de uma rede de dados. Tais sistemas são utilizados pelos servidores lotados no Fórum Clóvis Beviláqua, Tribunal de Justiça do Estado do Ceará e 26 (vinte e seis) unidades do Judiciário Cearense entre elas, Juizado Especial Cível e Criminal – JECC e Escola Superior da Magistratura do Estado do Ceará – ESMEC. O acesso é provido por meio da GigaFOR, projeto de infraestrutura baseado nas Redes Comunitárias de Educação e Pesquisa (Rede COMEP) do Ministério da Ciência, Tecnologia e Inovação, com uso de fibras ópticas e conecta órgãos dos poderes executivos legislativo e judiciário em todo o estado do Ceará.

A GigaFOR situa-se na Região Metropolitana de Fortaleza e interliga cerca de 20 pontos de diversas instituições da metrópole através de uma rede óptica de alta velocidade de mais de 72 km. Em sua concepção, o projeto do Cinturão Digital do Ceará pretende oferecer infraestrutura de forma a possibilitar que até o final de 2017, 105 (cento e cinco) municípios possam utilizar os recursos de conectividade. A previsão é que para o ano de 2016 sejam contempladas com o projeto, 08 (oito) municípios. Para que as demais unidades presentes no interior do Estado do Ceará venham a usufruir desse ambiente de conectividade em expansão, há em concomitância a necessidade de expandir o ambiente de tecnologia VPN do Judiciário.

A aquisição dos equipamentos acima mencionados foi contemplada através da celebração do contrato CT Nº 73/2010, celebrado com a empresa Lanlink Informática LTDA. Dada a dilação temporal do fornecimento dos mesmos, a atual infraestrutura de conectividade de firewall encontra-se sem os serviços de garantia e suporte, o que pode implicar em riscos de segurança no que diz respeito à trafegabilidade e a integridade dos dados, não sendo possível a extensão/contratação do serviço pois os equipamentos adquiridos estão em end-of-life (é um termo que se refere aos produtos fornecido aos clientes, que indica que o produto está no fim da sua vida útil ou descontinuado). Em caso de falha, por não estarem cobertos pela política de suporte de seus respectivos fabricantes, tais equipamentos podem vir a gerar a indisponibilidade dos Sistemas Judiciais e Administrativos citados anteriormente.

O Poder Judiciário do Estado do Ceará pretende expandir a utilização do uso do Cinturão Digital do Governo do Ceará para as comarcas do interior, tal utilização necessitará de

controles centralizados para controlar o tráfego de rede entre o cinturão, as comarcas e os ambientes computacionais do Tribunal de Justiça do Estado do Ceará (TJCE) e do Fórum Clóvis Beviláqua (FCB).

Para manter o nível adequado de segurança da informação, há a necessidade de manter e expandir o controle de acesso de usuários e de outros aplicativos a sites maliciosos, além de garantir que as informações existentes neste Poder estejam protegidas contra ataques maliciosos, no que tange às ameaças provenientes de ataques internos e externos.

O objetivo em adquirir a solução integrada de perímetro de segurança da informação consiste em substituir os 03 concentradores de Firewalls, os 02 (dois) equipamentos de IPS todos adquiridos no contrato CT Nº 73/2010 e defasados tecnologicamente, incluindo também solução para interligar as comarcas que utilizam a rede do TJCE e que utilizarão o Cinturão Digita

Como o prazo de garantia/suporte dos equipamentos adquiridos já expirou e os mesmos não dispõem mais de serviço de garantia/suporte pois foram descontinuados pelo fabricante, faz-se necessário adquirir solução integrada de perímetro de segurança da informação para atender a atual demanda e continuar a oferecer os serviços já citados acima, propiciando ganhos na segurança, estabilidade, disponibilidade e desempenho dos Sistemas Administrativos e Judiciais que utilizam a solução atual.

2.3. Resultados a serem Alcançados com a Contratação

- Manutenção e controle do tráfego de rede;
- Filtrar conteúdo Web e de dados;
- Prevenir a rede interna contra ameaças cibernéticas digitais;
- Estabelecer canal de comunicação seguro através da VPN;
- Aumentar a proteção da rede interna contra possíveis tentativas de acesso indevido;
- Implementar mecanismos de proteção, prevenção de intrusão.

2.4. Levantamento das alternativas

Solução Única - Contratação de empresa especializada em tecnologia da informação para fornecimento de solução de servidores para datacenter, incluindo serviços de instalação e garantia pelo período de 60 (sessenta) meses.			
Entidade	Ata de Registro de Preço da Justiça Federal do Paraná e empresas fornecedoras de propostas, obtidas através de pesquisa mercadológica.		
Descrição	Contratação de empresa especializada para o fornecimento de solução de segurança de perímetro com características de Next Generation Firewall, instalação, configuração, migração, garantia e suporte técnico pelo período de 60 (sessenta) meses.		
Fornecedor	Compwire; FastHelp; NivaTI; TrustControl; Teltec Solutions.	**Valor**	**R$ 2.680.389,92**

OBS.:

– AS EMPRESAS EM SUAS PROPOSTAS UTILIZARAM O VALOR UNITÁRIO PARA O PERÍODO DE 12 MESES (MENSAL). OBJETIVANDO ADEQUAR OS CÁLCULOS DE MÉDIA MERCADOLÓGICA, REALIZAMOS A CONVERSÃO DOS VALORES UNITÁRIOS DE MESES (MENSALMENTE) PARA ANO (ANUALMENTE). OU SEJA, DE 60 MESES PARA 5 ANOS PARA TODAS AS OUTRAS EMPRESAS. O MESMO ACONTECE NA ARP DA JFPR.

– FÓRMULA: (60 MESES / 12) * O VLR. UNIT.

2.5. Referência aos estudos preliminares

2.5.1. O resultado da realização dos Estudos Preliminares encontram-se apresentados através dos seguintes documentos: Análise de Viabilidade da Contratação; Plano de Sustentação; Planejamento Estratégico da Contratação e Plano de Riscos.

2.6. Alinhamento estratégico

ID	Objetivo Estratégico do Requisitante	ID	Necessidades Elencadas no PDTI
01	Garantir a segurança da informação	N132	Contratação de Firewall.
02	Garantir a infraestrutura de TIC	N132	Contratação de Firewall.

2.7. Justificativa da Solução Escolhida

Das soluções apresentadas e ofertadas no mercado, foi verificado que a solução poderia ser adquirida de duas formas: a oferta da aquisição dos equipamentos, licenciamento/ativação de software com garantia, bem como, a terceirização dos serviços em Segurança de perímetro na forma de outsorcing, incluindo equipamentos, softwares e sua operacionalização, assim como, definição de regras, gestão dos serviços e processos envolvidos.

Após pesquisas na Internet através de sites buscadores, identificamos vários Editais (Pregão Eletrônico N. 7/2015 do TJSC, Pregão Eletrônico N. 101/2013 do BACEN, Pregão Eletrônico N. 62/2014 do TJPR, Pregão Eletrônico N. 3/2016 da CAESB), que tratam de soluções de perímetros, observamos que a prática nos órgãos públicos têm sido a aquisição dos equipamentos com garantia.

No arquivo publicado através do link: http://www.governoeletronico.gov.br/eixos-de-atuacao/governo/sistema-de-administracao-dos-recursos-de-tecnologia-da-informacao-sisp/ncti-nucleo-de-contratacoes-de-tecnologia-da-informacao/consulta-licitacoes-de-ti, com data base de dados do mês de junho de 2016, para ativos de rede, identificamos 64 itens relacionados a Aquisição de solução em segurança de perímetro, onde apenas uma foi sob a forma de outsorcing.

Uma possível desvantagem do *outsourcing* é justamente a falta de segurança. Apesar dos benefícios, não podemos ignorar o fato de que todos os dados do TJCE estarão abertos a outra corporação completamente independente da sua, e por isso não há garantias de que essas informações não serão utilizadas de forma inadequada.

Além disso, foi aprovada a Política de Segurança da Informação do TJCE através da Resolução do Órgão Especial Nº 25/2016 de 01/09/2016 e que esta diz que as informações geradas no âmbito do Poder Judiciário do Estado do Ceará são de sua propriedade e devem ser adequadamente protegidas e utilizadas. Ora, caso a contratação fosse sob a forma de *outsourcing* as informações poderiam ficar desprotegidas, pois a solução seria gerenciada por terceiros e poderia ocorrer vazamento de informações ou roubo de dados.

Do ponto de vista da Segurança da Informação, todas as informações que trafegam na rede do TJCE e necessitam transpor ao ambiente externo, passam por um ponto único e sob a gestão e operacionalização do TJCE, desta forma entendemos que devido as regras de segurança hoje implementadas nos firewall, bem como, as regras que pretendemos implementar para o bloqueio de sites, gerenciamento de aplicações, verificações de vulnerabilidades e a gestão do processo de perímetro de segurança da informação de forma centralizada, não é recomendado a contratação da solução de segurança de perímetro sob a forma de outsourcing.

Desta forma, descartamos a solução 2 que trata o objeto como "Alocação de solução integrada de software e hardware".

Optamos pela solução 1 onde hoje em dia é a mais utilizada por órgãos do Brasil inteiro, sendo realizado registro de preços através de pregão eletrônico pelo TJCE.

Para interligação das comarcas do interior e o TJCE através do Cinturão Digital é preciso da infraestrutura de última milha de fibra que é de responsabilidade da ETICE (Empresa de Tecnologia do Ceará). Conforme o planejamento da ETICE, está previsto a entrega de 8 (oito) comarcas com infraestrutura de última milha de fibra até o final de 2016 e o restante ao longo do ano de 2017. Também temos que, por questões de falta de

infraestrutura (conexões lógicas e elétricas) do data center do FCB para receber novos equipamentos concentradores de firewall, parte dos itens para atender a solução deverão ser adquiridos em 2016 e a outra parte em 2017, quando a infraestrutura estiver disponível. A realização de pregão eletrônico proporcionará ao TJCE adquirir os itens de forma parcelada de acordo com o planejado para os anos de 2016 e 2017.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. Fornecimento de appliances com características de Next Generation Firewall, compreendendo aquisição de equipamentos conforme subitem **2.1.1**:

4. ESPECIFICAÇÃO TÉCNICA

4.1. Compreende a solução de segurança de perímetro o fornecimento de:

4.1.1. Appliances Next Generation Firewall para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo, licenciado/ativado para funcionamento com as funcionalidades de Controle de Aplicações, Prevenção de Ameaças, Proteção IPS, Proteção Antivírus e Antispyware, Análise de Malwares Modernos, Filtro de URL, Controle de Transferência de Arquivos, Controle de Tráfego, De-criptografia SSL, Módulo VPN, Roteamento, NAT, Gerenciamento e com garantia durante 60 (sessenta) meses conforme descrito no **ANEXO I – ESPECIFICAÇÕES TÉCNICAS e ANEXO II – GARANTIA E SUPORTE TÉCNICO**. Bem como sua instalação, configuração e migração, conforme **ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO**.

5. MODELO DE FORNECIMENTO DE BENS

5.1. Justificativa para Parcelamento do Objeto

5.1.1. Dada a especificidade da solução, o parcelamento do objeto torna-se desnecessário. Tal procedimento não enseja nenhum ganho de competitividade ou benefício

financeiro ao TJCE.

5.2. Metodologia de Trabalho

ID	DEMANDA PREVISTA	FORMA DE FORNECIMENTO	JUSTIFICATIVA
1	Solução de Plataforma de Segurança em cluster, no mínimo: 02 (dois) Firewalls de Próxima, para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo Geração. Serviço de instalação e configuração devem estar incluídos.	Conforme especificado nos seus referidos anexos.	Conforme praticado no mercado e ao que melhor se adéqua ao TJCE.
2	Garantia da Solução de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em Português por autorizada credenciada e com serviço de suporte técnico remoto por 12 meses a ser prestado pela CONTRATADA.		
3	Software com licenciamento de uso perpétuo para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução em cluster. Com no mínimo, 60 meses de suporte.		
4	Módulo de Interface 1000BASE-T		
5	Módulo de interface 10GBASE-SR		
6	Software para Gerenciamento da Solução de Segurança em cluster.		
7	Garantia do Software para Gerenciamento da Solução de Segurança em cluster com Suporte Oficial do fabricante, através da Contratada, 24x7 fornecido no Brasil em Português. Com no mínimo, 60 meses de suporte.		

6. ELEMENTOS PARA GESTÃO DO CONTRATO

6.1. Papeis e Responsabilidade

ID	Papel	Entidade	Responsabilidade
1	**Fiscal Técnico**	**Coordenador(a) de Suporte Técnico**	Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os Critérios de Aceitação definidos em contrato; Identificação de não conformidade com os termos contratuais; Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da contratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato); Comunicar por escrito, ao gestor do contrato, qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar à aplicação de sanção ou à rescisão contratual; Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato; Realizar pessoalmente a medição dos serviços contratados; Recusar serviço ou fornecimento irregular ou em desacordo com condições previstas em edital, na proposta da contratada e no

			contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados; Averiguar se é o contratado quem executa o contrato e certificar-se de que não existe cessão ou subcontratação fora das hipóteses legais; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato, em conjunto com o Fiscal Requisitante quando solicitado pelo Gestor do Contrato; Atestar a efetiva realização do objeto contratado para fins de pagamento das faturas correspondentes;
2	**Fiscal Requisitante do Contrato**	**Chefe do Serviço de Segurança da Informação**	Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os Critérios de Aceitação definidos em contrato, em conjunto com o Fiscal Técnico quando solicitado pelo Gestor do Contrato; Identificação de não conformidade com os termos contratuais, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Verificação da manutenção da necessidade, economicidade e oportunidade da contratação; Verificação de manutenção das condições elencadas no Plano de Sustentação (Documento elaborado no planejamento da con-

			tratação, que visa garantir a continuidade do negócio durante e após a entrega da Solução de Tecnologia da Informação, bem como após o encerramento do contrato), em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle da qualidade dos materiais, serviços e equipamentos a serem aplicados nos serviços, em conjunto com o Fiscal Técnico; Verificar o cumprimento das normas trabalhistas por parte do contratado, a exemplo da jornada de trabalho, limitações de horas extras, descanso semanal, bem como da obediência às normas de segurança do trabalho, a fim de evitar acidentes com agentes administrativos, terceiros e empregados do contrato, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Receber e dirimir reclamações relacionadas à qualidade de serviços prestados, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato; Comunicar por escrito, ao gestor do contrato, qualquer falta cometida pela empresa contratada, seja por inadimplemento de cláusula ou condição do contrato, ou por serviço executado de forma inadequada, fora do prazo, ou mesmo não realizado, formando o dossiê das providências adotadas para fins de materialização dos fatos que poderão levar a aplicação de sanção ou à rescisão contratual, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato;

			Sugerir ao gestor do contrato a aplicação de penalidades nos casos de inadimplemento parcial ou total do contrato, em conjunto com o Fiscal Técnico, quando solicitado pelo Gestor do Contrato.
3	**Fiscal Administrativo**	**Coordenador (a) da Divisão de Gestão Administrativa de TI**	Certificar-se do correto cálculo e recolhimento das obrigações trabalhistas, previdenciárias e tributárias decorrentes do contrato; Efetuar o controle da vigência, realizando comunicado ao fiscal técnico em tempo hábil, uma vez que este deverá controlar os prazos de execução, necessidades de prorrogações ou nova contratação, ficando o fiscal administrativo responsável pelo controle da época de reajustamento dos preços contratados, tomando as providências cabíveis em tempo hábil junto à Divisão Central de Contratos e Convênios do TJCE, quando necessário; Verificar se a empresa contratada cumpriu com a garantia prevista no contrato.
4	**Gestor do Contrato**	**Secretário(a) de Tecnologia da Informação**	Manter registro próprio, atualizado, das ocorrências relacionadas à execução do contrato; Acompanhar o cumprimento do cronograma de execução e dos prazos previstos; Determinar à contratada a regularização das falhas ou defeitos observados, assinalando prazo para correção; Relatar, por escrito, à autoridade competente do órgão responsável, a inobservância de cláusulas contratuais ou quaisquer ocorrências que possam trazer dificuldades, atrasos, defeitos e prejuízos à execução da

			avença, em especial os que ensejarem a aplicação de penalidades; Comunicar à autoridade competente do órgão responsável, apresentando as devidas justificativas, a eventual necessidade de acréscimos ou supressões de serviços, materiais ou equipamentos, identificadas no curso das atividades de fiscalização; Solicitar à contratada a substituição de empregado ou preposto da contratada e aprovar, previamente, mediante termo juntado ao processo, a substituição de iniciativa da contratada, quando assim exigir o contrato; Receber, definitivamente, por meio de ateste na nota fiscal/fatura ou documento equivalente, devidamente discriminado, obras, serviços e materiais; Acompanhar o prazo de vigência do contrato e manifestar-se, quando provocado pela Administração, sobre os aspectos de oportunidade, conveniência, razoabilidade e economicidade administrativa de se realizar alteração, prorrogação ou rescisão do contrato, anexando, quando for o caso, documentação comprobatória.

6.2. Deveres e Responsabilidades do Contratante

6.2.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Fornecimento e/ou Serviço;

6.2.2. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal n.º 8.666/1993 e suas alterações;

6.2.3. Notificar a contratada de qualquer irregularidade decorrente da execução do

objeto contratual.

6.2.4. Efetuar os pagamentos devidos à contratada nas condições estabelecidas em contrato.

6.2.5. Aplicar as penalidades previstas em lei e neste instrumento.

6.3. Deveres e Responsabilidades da Contratada

6.3.1. Constituem obrigações da CONTRATADA, além de outras previstas em Contrato e na legislação pertinente, as seguintes:

6.3.1.1. Orientar tecnicamente os responsáveis pela operação dos bens, fornecendo os esclarecimentos necessários ao seu perfeito funcionamento.

6.3.2. Proceder à entrega dos bens, devidamente embalados, de forma a não serem danificados durante a operação de transporte e de carga e descarga, assinalando na embalagem a marca, destino e, quando for o caso, número da Licença de Importação ou documento equivalente, com as especificações detalhadas ou documento equivalente, para conferência.

6.3.3. Efetuar a entrega dos bens:

6.3.3.1. De acordo com as especificações e demais condições estipuladas neste documento;

6.3.4. Efetuar a prestação dos serviços:

6.3.4.1. Instalação, configuração e migração de acordo com as especificações e demais condições estipuladas contratualmente.

6.3.5. Manter, durante a execução do contrato, todas as condições de habilitação e de qualificação exigidas na licitação.

6.3.6. Realizar testes e corrigir defeitos nos bens, inclusive com a sua substituição quando necessário, sem ônus para o CONTRATANTE, durante o período de garantia.

6.3.7. Responder por todos os ônus referentes a entrega dos bens e serviços ora contratados, desde os salários dos seus empregados, como também os encargos trabalhistas, previdenciários, fiscais e comerciais, que venham a incidir sobre o contrato.

6.3.8. Entregar os bens e realizar a prestação dos serviços contratados no local indicado pelo CONTRATANTE.

6.3.9. Responsabilizar-se:

6.3.9.1. Por quaisquer acidentes na entrega dos bens e, ainda, por fatos de que resultem as destruições ou danificações dos mesmos, estendendo-se essa responsabilidade até a assinatura do "Termo de Recebimento Definitivo dos Bens e a integral liquidação de indenização caso devida a terceiros.

6.3.9.2. Pelo pagamento de seguros, impostos, taxas e serviços, encargos sociais e trabalhistas, e quaisquer despesas referentes aos bens, inclusive licença em repartições públicas, registros, publicações e autenticações do contrato e dos documentos a ele relativos, se necessário.

6.3.10. Executar o objeto em conformidade com as condições deste instrumento.

6.3.11. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no § 1º, do art. 65, da Lei Federal nº 8.666/1993, tomando-se por base o valor contratual.

6.3.12. Responsabilizar-se pelos danos causados diretamente ao 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 o contratante proceder à fiscalização ou acompanhar a execução contratual.

6.3.13. Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução do contrato, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo

obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.

6.3.14. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitantes pelo contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

6.3.15. Substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações do objeto, antes da emissão do Termo de Recebimento Definitivo, no prazo de 15 (quinze) dia(s), contados da sua notificação.

6.3.16. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.

6.3.17. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização do contratante.

6.4. Forma de Acompanhamento do Contrato

ID	Etapa/Fase/Item	Forma de Acompanhamento
1	Entrega dos itens	Serão conferidos se estão de acordo com as especificações contratuais, pela equipe da Gerência de Infraestrutura de T.I do TJCE ou pela equipe da Coordenadoria de Suporte Técnico do TJCE. O não cumprimento das especificações está sujeito a sanções previstas neste Termo de Referência. O TJCE enviará um ofício a CONTRATADA notificando-a sobre o não cumprimento das especificações apontadas neste documento.

6.5. Metodologia de Avaliação da Qualidade

Etapa/Fase/Item	Método de Avaliação
Entrega do Plano de	Deverá estar de acordo com as especificações técnicas descritas em

Instalação	contrato. Deverá ser entregue no prazo e local determinado em contrato.
Durante a entrega da solução.	A solução deverá estar de acordo com as especificações descritas em contrato. Deverá ser entregue no prazo e local determinado em contrato.
Instalação, Configuração e Migração	Deverá estar de acordo com as especificações técnicas descritas em contrato. Deverá ser entregue no prazo e local determinado em contrato.
Durante a Garantia	Durante a prestação do serviço de garantia, será avaliado o cumprimento dos prazos de solução dos chamados e a conformidade técnica dos softwares e hardwares substituídos.
Recebimento do Objeto	O Objeto será recebido: **provisoriamente**, em até 10 (dez) dias da entrega do objeto, mediante Termo de Recebimento Provisório, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito pelo(s) fiscal(is) do contrato. **definitivamente**, sendo expedido termo de recebimento definitivo, em até 10 (dez) dias do recebimento provisório, após verificação da qualidade e da quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e, consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

6.6. Fiscalização

6.6.1. A execução do Contrato será acompanhada e fiscalizada pelo Fiscal Técnico do Contrato, especialmente designado. Sem prejuízo da plena responsabilidade da Contratada perante o TJCE e/ou a terceiros, os serviços estarão sujeitos a mais ampla e irrestrita fiscalização, a qualquer hora e em todos os locais. A presença do Fiscal Técnico do Contrato não diminui a responsabilidade da empresa por quaisquer irregularidades resultantes de imperfeições técnicas e não implicam corresponsabilidade do TJCE ou do Fiscal.

6.6.2. O Fiscal Técnico monitora os riscos inerentes à execução dos serviços. Para tanto, registra todas as ocorrências relacionadas à execução do contrato, determinando

o que for necessário à regularização das falhas. Caso existam falhas que requeiram a aplicação de sanções, o Fiscal comunica ao Gestor do Contrato para que tome as devidas providências. Todas as decisões e ações que ultrapassem a competência do Fiscal Técnico devem ser solicitadas ao Gestor do Contrato em tempo hábil para adoção de medidas cabíveis.

6.6.3. Ao Fiscal Técnico fica assegurado o direito de exigir o cumprimento de todos os itens constantes do Termo de Referência, do Edital, da proposta e das cláusulas do Contrato.

6.6.4. Eventuais irregularidades deverão ser comunicadas pela Contratada, por escrito, ao Fiscal Técnico com os esclarecimentos julgados necessários e as informações sobre possíveis paralisações de serviços. Devem ser apresentados relatórios técnicos ou justificativas a serem apreciadas e decididas pelo Gestor do Contrato.

6.7. Estimativa do Volume de Bens

ITEM	DESCRIÇÃO	UNIDADE	QTD
1	Solução de Plataforma de Segurança em cluster, no mínimo: 02 (dois) Firewalls de Próxima, para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo Geração. Serviço de instalação e configuração devem estar incluídos.	UND	1
2	Garantia da Solução de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em Português por autorizada credenciada e com serviço de suporte técnico remoto por 12 meses a ser prestado pela CONTRATADA.	Mês	60
3	Software com licenciamento de uso perpétuo para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução em cluster. Com no mínimo, 60 meses de suporte.	Licença	1
4	Módulo de Interface 1000BASE-T	UND	2
5	Módulo de interface 10GBASE-SR	UND	14

6	Software para Gerenciamento da Solução de Segurança em cluster.	UND	1
7	Garantia do Software para Gerenciamento da Solução de Segurança em cluster com Suporte Oficial do fabricante, através da Contratada, 24x7 fornecido no Brasil em Português. Com no mínimo, 60 meses de suporte.	Mês	60

6.8. Prazos e Condições

6.8.1. O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento, nos endereços, prazos e horários previstos nos subitens seguintes:

6.8.1.1. Prazo e Local para a entrega da solução:

6.8.1.1.1. O prazo de entrega de produtos deverá ocorrer em um prazo não superior 90 (noventa) dias corridos a partir da data de assinatura do contrato;

6.8.1.1.2. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

6.8.1.1.3. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação;

6.8.1.1.4. O local de entrega da solução é:

6.8.1.1.4.1. **TJCE** – Av. General Afonso Albuquerque Lima, S/N. – Cambeba, CEP: 60822-325 – **Almoxarifado**. Em data e horário previamente agendados com o contratante, no horário de funcionamento das 08:00 às 18:00 em dias úteis (segunda a sexta-feira);

6.8.1.1.5. Caso os equipamentos sejam diferentes das especificações ou apresentem defeitos serão considerados não entregues e a contagem do prazo de entrega não

será interrompida devido à rejeição dos mesmos.

6.8.1.1.6. 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 entrega e aceitos pelo CONTRATANTE, não serão considerados como inadimplemento contratual.

6.8.1.1.7. Caso aconteça algum fato superveniente não motivado pela contratada, o fato deve ser informado ao Contratante, mediante ofício protocolado na sede do Contratante.

6.8.1.1.8. O não cumprimento do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior à solicitada implicará em aplicação das penalidades previstas neste Termo de Referência.

6.8.1.1.9. Serão aceitos apenas equipamentos novos e sem uso. Não serão aceitos equipamentos re-manufaturados, NFR (Not For Resale) ou de demonstração. Os equipamentos deverão ser entregues nas caixas lacradas pelo fabricante, não sendo aceitos equipamentos com caixas violadas;

6.8.1.1.10. Em caso de dúvida ou divergência na comprovação da especificação técnica, o TJCE poderá solicitar amostra do equipamento ofertado, sem ônus ao processo, para comprovação técnica de funcionalidades. Esta amostra deverá ocorrer em até 15 (quinze) dias úteis após a solicitação. Para a amostra, a empresa deverá apresentar o mesmo modelo do equipamento ofertado na proposta, com técnico certificado na solução para configuração e comprovação dos itens pendentes, nas dependências do TJCE

6.9. DO RECEBIMENTO

6.9.1. Quanto ao recebimento:

6.9.1.1. O TJCE receberá provisoriamente (Termo de Recebimento Provisório) em um prazo não superior a 10 (dez) dias úteis, e definitivamente (Termo de Recebimento Definitivo) em um prazo não superior a 10 (dez) dias úteis, contados a partir da data de

assinatura do Termo de Recebimento Provisório, verificando a conformidade e qualidade dos produtos ofertados quanto às exigências contidas no Contrato;

6.9.1.2. O aceite do bem somente será dado após comprovação da entrega e o efetivo cumprimento de todas as exigências da presente especificação técnica;

6.9.1.3. Será consultado, diretamente no site do fabricante, manuais e toda documentação pública disponível para comprovação do pleno atendimento aos requisitos estabelecidos neste documento;

6.10. Condições para Pagamento

6.10.1. Os pagamentos serão realizados através de depósito bancário preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento definitivo do objeto constante de cada uma das Ordens de Fornecimento de Bens e/ou Ordem de Serviço emitidas pelo Tribunal de Justiça, mediante apresentação de fatura/nota fiscal, atestada pelo setor competente deste Tribunal de Justiça, e também de apresentação de certidões que comprovem a regularidade da empresa com o fisco Federal, Estadual e Municipal, FGTS e INSS e débitos trabalhistas;

6.10.2. Constatada alguma situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE;

6.10.3. Não havendo regularização ou sendo a defesa considerada improcedente, o TJCE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

6.10.4. Persistindo a irregularidade, o TJCE deverá adotar as medidas necessárias a

rescisão do contrato e o Cancelamento da Ata de Registro de Preços nos autos do processo administrativo correspondente, assegurada a CONTRATADA a ampla defesa;

6.10.5. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato e o cancelamento da Ata de Registro de Preços, caso a CONTRATADA não regularize sua situação;

6.10.6. Por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado pela máxima autoridade do TJCE, não será rescindido o contrato e cancelada a Ata de Registro de Preços em execução com a CONTRATADA inadimplente;

6.10.7. A(s) nota(s) fiscal(is) /fatura(s) deverá(ão) ser emitida(s) em nome do Fundo Especial de reaparelhamento e Modernização do Judiciário – FERMOJU, CNPJ N.º 41.655.846/0001-47;

6.10.8. O Tribunal de Justiça do Ceará não se responsabiliza por qualquer despesa bancária, nem por qualquer outro pagamento não previsto no instrumento contratual;

6.10.9. Havendo erro no documento de cobrança ou outra circunstância que desaprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado, até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

6.11. Garantia e Suporte Técnico

6.11.1. Conforme **ANEXO II – GARANTIA E SUPORTE TÉCNICO**.

6.12. Propriedade, Sigilo, Restrições

6.12.1. Todas as informações obtidas ou extraídas pela CONTRATADA quando da execução do objeto deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a mesma zelar por si e por seus sócios, empregados e subcontratados pela manutenção do sigilo absoluto sobre os dados, informações,

documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso em razão da execução do contrato;

6.12.2. A obrigação assumida de Confidencialidade permanecerá válida durante e também após o período de vigência contratual;

6.12.3. A CONTRATADA deverá assinar o **ANEXO IV – MODELO DE TERMO DE CIÊNCIA – TCI** e o **ANEXO V – MODELO DE TERMO DE COMPROMISSO – TC**;

6.12.4. Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a CONTRATADA exigirá de todos os seus empregados, colaboradores ou prestadores de serviços, que façam parte, a qualquer título, da equipe executante do Objeto deste Documento, a assinatura do Termo de Confidencialidade, onde o signatário declara-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

6.13. Mecanismos Formais de Comunicação

ID	Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
1	Emissão da Ordem de fornecimento	Contratante	Contratada	Ordem de fornecimento	Quando demandado pela SETIN.
2	Emissão da Nota de Empenho	Contratante	Contratada	Nota de empenho	Quando demandado pela SETIN.
3	Abertura de chamados da garantia. Dirimir dúvidas e prestar esclarecimentos acerca de itens presentes no contrato firmado;	Contratante	Contratada	E-mail, telefone e site na internet	Sempre que necessário.

4	Registro das reuniões realizadas entre o contratante e a contratada.	Contratante	Contratada	Ata de reunião	Sempre que houver reunião entre as partes.
5	Relato de alguma ocorrência contratual através de Ofício por correspondência.	Contratante	Contratada	Comunicação formal	Sempre que houver falha no atendimento a algum item do contrato ou quando necessário.
6	Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, e-mail, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*Portable Document Format*): documento em formato portável.	Quando necessário

7. ESTIMATIVA DE PREÇO

ITEM	DESCRIÇÃO	UNIDADE	QTD	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Plataforma de Segurança em cluster, no mínimo: 02 (dois) Firewalls de Próxima, para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo Geração. Serviço de instalação e configuração devem estar incluídos.	UND	1	R$ 680.745,60	R$ 680.745,60
2	Garantia da Solução de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em	Mês	60	R$ 112.596,29	R$ 562.981,45

	Português por autorizada credenciada e com serviço de suporte técnico remoto por 12 meses a ser prestado pela CONTRATADA.				
3	Software com licenciamento de uso perpétuo para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução em cluster. Com no mínimo, 60 meses de suporte.	Licença	1	R$ 218.651,59	R$ 1.093.257,95
4	Módulo de Interface 1000BASE-T	UND	2	R$ 11.819,00	R$ 23.638,00
5	Módulo de interface 10GBASE-SR	UND	14	R$ 14.244,78	R$ 199.426,92
6	Software para Gerenciamento da Solução de Segurança em cluster.	UND	1	R$ 41.175,00	R$ 41.175,00
7	Garantia do Software para Gerenciamento da Solução de Segurança em cluster com Suporte Oficial do fabricante, através da Contratada, 24x7 fornecido no Brasil em Português. Com no mínimo, 60 meses de suporte.	Mês	60	R$ 15.833,00	R$ 79.165,00
				VALOR GLOBAL	**** Erro na expressão ****

8. ADEQUAÇÃO ORÇAMENTÁRIA

FONTE	Tribunal de Justiça do Estado do Ceará		
Programa	500 – Gestão e Manutenção do TJ		
Período	Natureza	Ação 21809 – Manutenção e Funcionamento de TI – TJ – 1º Grau	Valores
Previsto para 2018	Investimento	Solução de Plataforma de Segurança em cluster, no mínimo: 02 (dois) Firewalls de Próxima, para operar em alta disponibilidade em modo ativo-passivo ou ativo-ativo Geração. Serviço de instalação e configuração devem estar incluídos.	R$ 680.745,60
		Garantia da Solução de Segurança em cluster com Suporte Oficial 24x7 fornecido no Brasil em Português por autorizada credenciada e com serviço de suporte técnico remoto por 12 meses a ser prestado pela CONTRATADA.	R$ 562.981,45
		Software com licenciamento de uso perpétuo para prevenção de Intrusão(IPS), proteção de Malware e Exploit, spyware, filtro de URL e Detecção e prevenção de malware de dia zero para a solução em cluster. Com no mínimo, 60 meses de suporte.	R$ 1.093.257,95

		Módulo de Interface 1000BASE-T	R$ 23.638,00
		Módulo de interface 10GBASE-SR	R$ 199.426,92
		Software para Gerenciamento da Solução de Segurança em cluster.	R$ 41.175,00
		Garantia do Software para Gerenciamento da Solução de Segurança em cluster com Suporte Oficial do fabricante, através da Contratada, 24x7 fornecido no Brasil em Português. Com no mínimo, 60 meses de suporte.	R$ 79.165,00
		VALOR GLOBAL	**** Erro na expressão ****

9. Sanções Aplicáveis

9.1.1. Com fundamento no art. 7 da Lei N. 10.520/2002 e, subsidiariamente, nos artigos 86 e 87 da Lei N. 8.666/1993, a CONTRATADA ficará sujeita, assegurada prévia e ampla defesa, as seguintes penalidades:

9.1.2. Advertência;

9.1.3. Multas, estipuladas na forma a seguir:

9.1.4. Multa diária de 0,3% (três décimos por cento), no caso de atraso na entrega de qualquer equipamento ou da conclusão da prestação dos serviços, até o 30º (trigésimo) dia, sobre o valor do item entregue em atraso.

9.1.5. Multa de 1% (um por cento), no caso de atraso na execução do objeto contratual

superior a 30 (trinta) dias, sobre o valor do item entregue em atraso. A aplicação da presente multa não exclui a aplicação da multa prevista na alínea anterior;

9.1.6. Multa diária de 0,1% (um décimo por cento) sobre o valor do item entregue em atraso, em caso de descumprimento das demais cláusulas contratuais, elevada para 0,3% (três décimos por cento) em caso de reincidência limitado a 10%;

9.1.7. Multa de 10% (dez por cento) sobre o valor do contrato, no caso de desistência da execução do objeto ou rescisão contratual não motivada pelo CONTRATANTE.

9.1.8. A CONTRATADA estará ainda sujeita a:

9.1.9. Impedimento de licitar e contratar com o Estado do Ceará e descredenciamento do SICAF, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas no contrato e das demais penalidades.

9.1.10. DECLARAÇÃO DE INIDONEIDADE para licitar e contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade;

9.1.11. RESCISÃO, nos casos previstos no art.78 da Lei nº 8.666/93.

9.1.12. Ao TJCE será assegurado, após regular processo administrativo, utilizar a garantia para permitir a compensação da multa aplicada. Se a multa for de valor superior ao valor da garantia prestada, além da perda desta, responderá a Contratada pela sua diferença, a qual será descontada dos pagamentos eventualmente devidos pela Administração ou ainda, quando for o caso, cobrada judicialmente;

9.1.13. As sanções acima descritas poderão ser aplicadas de forma distinta ou cumulativa;

9.1.14. Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA. As multas serão aplicadas sobre a garantia contratual e quando a mesma não for suficiente para a quitação integral da multa o restante será descontada nas notas fiscais da CONTRATADA;

9.1.15. A CONTRATADA terá prazo máximo de 05 (cinco) dias úteis contados do

recebimento da comunicação para apresentar as justificativas;

9.1.16. Caso não haja manifestação da CONTRATADA dentro desse prazo ou caso o CONTRATANTE entenda serem improcedentes as justificativas, serão aplicadas as penalidades previstas;

9.1.17. Caso ocorram divergências entre as justificativas apresentadas pela CONTRATADA e o atesto emitido pelo TJCE, o faturamento da parte incontroversa poderá ter o seu pagamento autorizado e os ajustes poderão ser realizados no período subsequente após a conclusão dos processos de apuração das irregularidades;

9.1.18. As notificações de multas e sanções são de responsabilidades da Divisão Central de Contratos e Convênios do TJCE que receberá dos setores responsáveis os relatórios com as ocorrências insatisfatórias que comprometam a execução do contrato.

10. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

10.1. Proposta de Preço

10.1.1. A proposta deverá conter obrigatoriamente os seguintes elementos:

10.1.2. Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais, expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;

10.1.3. Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;

10.1.4. Deve fazer menção ao número do pregão e do processo licitatório;

10.1.5. Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;

10.1.6. Deve conter na última folha o número do CNPJ da empresa;

10.1.7. Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;

10.1.8. Deverá conter a descrição detalhada do objeto, tais como: somente uma única marca, modelo, características do objeto, procedência e demais dados que a licitante julgar necessário;

10.1.9. Indicação do nome do banco, número da agência, número da conta-corrente, para fins de recebimento dos pagamentos;

10.2. Critérios de Seleção

10.2.1. Modalidade de Licitação

10.2.1.1. A modalidade de licitação escolhida deve ser o Pregão na forma eletrônica, considerando se tratar de bem comuns, nos termos da lei Federal n° 10.520/2002.

10.2.2. Tipo de Licitação

10.2.2.1. A licitação será do tipo menor preço. Os valores máximos aceitáveis, tanto unitários quanto global, estão descritos no item **7**.

11. GARANTIA CONTRATUAL

11.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive pagamento de multas eventualmente aplicadas, a CONTRATADA prestará garantia no percentual de 5% (cinco por cento) do valor total do contrato, podendo a CONTRATADA optar por qualquer das modalidades previstas no art. 56 da Lei 8.666/93, a saber:

11.1.1. Caução em dinheiro ou títulos da dívida pública, cuja exigibilidade não seja contestada pelo TJCE;

11.1.2. Quando se tratar de caução em dinheiro, deverá ser recolhido na Secretaria de Finanças do TJCE;

11.1.3. Seguro garantia;

11.1.4. Fiança bancária;

11.1.5. Em se tratando de fiança bancária, deverá constar do instrumento a expressa renúncia pelo fiador dos benefícios previstos nos artigos 827 e 835 do Código Civil;

11.1.6. Se o valor da garantia for utilizado em pagamento de qualquer obrigação, a Contratada deverá re-integralizar o seu valor, no prazo não superior a 10 (dez) dias, contados da data em que for notificada;

11.1.7. Quando a garantia for prestada sob a forma de Fiança Bancária, a Carta de Fiança deverá ter validade mínima igual ao prazo inicial do contrato, com expressa renúncia do fiador aos benefícios do art. 827 da Lei 10.406/02 – Código Civil, bem como conter cláusula de prorrogação automática, até que o Contratante confirme o cumprimento integral das obrigações da Contratada, devendo ainda estar reconhecidas em cartório as firmas dos garantes;

11.2. A não apresentação da garantia até a assinatura contratual ou sua apresentação em desacordo com o prazo fixado significará recusa à assinatura do contrato, ensejando aplicação das sanções previstas;

11.3. No caso de rescisão do contrato, por culpa da CONTRATADA, a garantia contratual será utilizada para cobrir todos prejuízos comprovados a que a CONTRATANTE vier a sofrer.

12. VIGÊNCIA CONTRATUAL

12.1. O prazo de vigência do contrato terá início na data da sua assinatura e vigorará:

12.1.1. Para o fornecimento da solução, até 90 (noventa) dias corridos após a data de assinatura do contrato.

12.1.2. Para a entrega dos Serviços de Instalação, Configuração e Migração, até 120 (cento e vinte) dias corridos após a data de assinatura do contrato.

12.1.3. Para a garantia e suporte técnico da solução a ser adquirida, por 60 (sessenta) meses contados a partir da emissão do termo de recebimento definitivo.

Equipe de Planejamento da Contratação	
Heldir Sampaio Silva – 9630 **Integrante Técnico**	Werley da Silva Almeida – 22722 **Integrante Administrativo**
Alexys Ribeiro Negreiros – 8201 **Integrante Requisitante**	Cristiano Henrique Lima de Carvalho – 5198 **Área de Tecnologia da Informação**
Fortaleza, 12 de Março de 2018	

13. APROVAÇÕES

Aprovo. Encaminha-se à Comissão Permanente de Licitação para iniciação de procedimento licitatório, segundo o art. 38 da Lei nº 8.666 de 21 de junho de 1993.

Autoridade Competente
Denise Maria Norões Olsen – 24667
Fortaleza, 12 de Março de 2018

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
TERMO DE REFERÊNCIA – TR

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

1 ESPECIFICAÇÕES MÍNIMAS

1.1 A plataforma de segurança deve possuir a capacidade e as características abaixo, por equipamento:

1.1.1 Throughput de 10 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

1.1.2 Throughput de 5 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

1.1.3 Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;

1.1.4 Não será aceito a comprovação de Throughput para funcionalidades de camada 7 (Controle de Aplicação e IPS, por exemplo), com tráfego UDP e/ou RFCs baseadas neste protocolo;

1.1.5 Quando as funcionalidades de controle de aplicação, IPS, antivírus e antispyware tiverem habilitadas de forma simultânea o tráfego deverá ser inspecionado de modo bidirecional com inspeção em toda a sessão do pacote, sem qualquer utilização de recurso de by-pass. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.

1.1.6 Suporte a, no mínimo, 2.000.000 de conexões simultâneas;

1.1.7 Suporte a, no mínimo, 110.000 novas conexões por segundo;

1.1.8 Fonte 120/240 AC ou DC, redundante e hot-swappble;

1.1.9 Cooler hot-swappble;

1.1.10 Disco Solid State Drive (SSD) redundante de, no mínimo, 240 GB.

1.1.11 16 (dezesseis) interfaces de rede 1/10 Gbps SFP. Sendo:

1.1.11.1 2 módulos de interface 1000BASE-T;

1.1.11.2 14 módulos de interface 10GBASE-SR.

1.1.12 2 (duas) Gbps interfaces dedicadas para alta disponibilidade;

1.1.13 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

1.1.14 1 (uma) interface do tipo console ou similar;

1.1.15 Suporte a, no mínimo, 100 (cem) roteadores virtuais;

1.1.16 Suporte a, no mínimo, 400 (quatrocentas) zonas de segurança;

1.1.17 Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos;

1.1.18 Estar licenciada para ou suportar sem o uso de licença, 4.000 (quatro mil) túneis de VPN IPSEC simultâneos;

1.2 Deve suportar, no mínimo, 25 sistemas virtuais lógicos (Contextos) no firewall Físico;

1.3 Os contextos virtuais devem suportar as funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;

1.4 Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

1.5 Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;

1.6 Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;

1.7 Deve estar coberto por garantia no Brasil do próprio fabricante dos equipamentos por 60 (sessenta) meses, compreendendo atualizações e correções de sistema operacional, atualização da base de aplicações, IPS, Antivírus, Anti – Spyware e demais funcionalidades requeridas neste processo e que dependem de atualização.

2 CARACTERÍSTICAS GERAIS

2.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

2.2 Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

2.3 As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

2.4 A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

2.5 O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

2.6 Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

2.7 O software deverá ser fornecido em sua versão mais atualizada;

2.8 Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

2.8.1 Suporte a 4094 VLAN Tags 802.1q;

2.8.2 Agregação de links 802.3ad e LACP;

2.8.3 Policy based routing ou policy based forwarding;

2.8.4 Roteamento multicast (PIM-SM);
2.8.5 DHCP Relay;
2.8.6 DHCP Server;
2.8.7 Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
2.8.8 Suportar sub-interfaces ethernet logicas.
2.8.9 Deve suportar os seguintes tipos de NAT:
  2.8.9.1 Nat dinâmico (Many-to-1);
  2.8.9.2 Nat dinâmico (Many-to-Many);
  2.8.9.3 Nat estático (1-to-1);
  2.8.9.4 NAT estático (Many-to-Many);
  2.8.9.5 Nat estático bidirecional 1-to-1;
  2.8.9.6 Tradução de porta (PAT);
  2.8.9.7 NAT de Origem;
  2.8.9.8 NAT de Destino;
  2.8.9.9 Suportar NAT de Origem e NAT de Destino simultaneamente;
2.8.10 Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
2.8.11 Deve implementar o protocolo ECMP;
2.8.12 Deve implementar balanceamento de link por hash do IP de origem;
2.8.13 Deve implementar balanceamento de link por hash do IP de origem e destino;
2.8.14 Deve implementar balanceamento de link através do método round-robin;
2.8.15 Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links.
2.8.16 Deve suportar o balanceamento de, no mínimo, quarto links;
2.8.17 Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
2.8.18 Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
2.8.19 Deve implementar o protocolo Link Layer Discovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
2.8.20 Enviar log para sistemas de monitoração externos, simultaneamente;
2.8.21 Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
2.8.22 Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
2.8.23 Proteção contra anti-spoofing;

2.8.24 Deve permitir bloquear sessoes TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
2.8.25 Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
2.8.26 Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.8.27 Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.8.28 Suportar a OSPF graceful restart;
2.8.29 Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;
2.8.30 O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos:
  2.8.30.1 Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
  2.8.30.2 Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
  2.8.30.3 Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
  2.8.30.4 Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
  2.8.30.5 Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;
2.8.31 Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
  2.8.31.1 Em modo transparente;
  2.8.31.2 Em layer 3;
2.8.32 A configuração em alta disponibilidade deve sincronizar:
  2.8.32.1 Sessões;
  2.8.32.2 Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
  2.8.32.3 Certificados de-criptografados;
  2.8.32.4 Associações de Segurança das VPNs;
  2.8.32.5 Tabelas FIB;
  2.8.32.6 O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.
2.8.33 As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH;

2.8.34 Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

3 CONTROLE POR POLÍTICA DE FIREWALL

3.1 Deverá suportar controles por zona de segurança.
3.2 Controles de políticas por porta e protocolo.
3.3 Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
3.4 Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
3.5 Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.
3.6 Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).
3.7 Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
3.8 Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
3.9 Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
3.10 Controle de inspeção e de-criptografia de SSH por política;
3.11 A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
3.12 A plataforma de segurança deve implementar espelhamento de tráfego decriptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
3.13 É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.
3.14 Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg;
3.15 Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo);
3.16 QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
3.17 Suporte a objetos e regras IPV6.
3.18 Suporte a objetos e regras multicast.
3.19 Deve suportar no mínimo três tipos de negação de tráfego nas políticas de firewall:
3.19.1 Drop sem notificação do bloqueio ao usuário;
3.19.2 Drop com opção de envio de ICMP;

3.19.3 Unreachable para máquina de origem do tráfego;

3.19.4 TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

3.20 Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

4 CONTROLE DE APLICAÇÕES

4.1 Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

4.1.1 Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

4.1.2 Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

4.1.3 Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http,gotomeeting, webex, evernote, google-docs, etc;

4.1.4 Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

4.1.5 Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

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

4.1.7 Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

4.1.8 Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros

conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

4.1.9 Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

4.1.10 Identificar o uso de táticas evasivas via comunicações criptografadas;

4.1.11 Atualizar a base de assinaturas de aplicações automaticamente;

4.1.12 Reconhecer aplicações em IPv6;

4.1.13 Limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos do LDAP/AD;

4.1.14 Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

4.1.15 Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

4.1.16 Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

4.1.17 Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

4.1.18 Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

4.2 A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

4.2.1 HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

4.3 O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

4.4 Deve alertar o usuário quando uma aplicação for bloqueada;

4.5 Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

4.6 Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos;

4.7 Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;

4.8 Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

4.9 Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;

4.10 Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

4.10.1 Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

4.10.2 Nível de risco da aplicação;

4.10.3 Categoria e sub-categoria de aplicações;

4.10.4 Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda, etc.

5 PREVENÇÃO DE AMEAÇAS

5.1 Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante;

5.2 Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

5.3 As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;

5.4 Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

5.5 Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

5.6 As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

5.7 Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;

5.8 Deve suportar granularidade nas politicas de IPS Antivírus e Anti-Spyware, possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

5.9 Deve permitir o bloqueio de vulnerabilidades;

5.10 Deve permitir o bloqueio de exploits conhecidos;

5.11 Deve incluir proteção contra-ataques de negação de serviços;

5.12 Deverá possuir os seguintes mecanismos de inspeção de IPS:

5.12.1 Análise de padrões de estado de conexões;

5.12.2 Análise de decodificação de protocolo;

5.12.3 Análise para detecção de anomalias de protocolo;

5.12.4 Análise heurística;

5.12.5 IP Defragmentation;

5.12.6 Remontagem de pacotes de TCP;
5.12.7 Bloqueio de pacotes malformados.

5.13 Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;

5.14 Detectar e bloquear a origem de portscans;

5.15 Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;

5.16 Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

5.17 Possuir assinaturas específicas para a mitigação de ataques DoS e DdoS;

5.18 Possuir assinaturas para bloqueio de ataques de buffer overflow;

5.19 Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

5.20 Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

5.21 Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos:
5.21.1 HTTP, FTP, SMB, SMTP e POP3;

5.22 É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;

5.23 Suportar bloqueio de arquivos por tipo;

5.24 Identificar e bloquear comunicação com botnets;

5.25 Deve suportar varias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

5.26 Deve suportar referencia cruzada com CVE;

5.27 Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
5.27.1 O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo.

5.28 Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;

5.29 Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

5.30 Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;

5.31 Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

5.32 Os eventos devem identificar o país de onde partiu a ameaça;
5.33 Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
5.34 Proteção contra downloads involuntários usando HTTP de arquivos executáveis;
5.35 Rastreamento de vírus em pdf;
5.36 Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.);
5.37 Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em politicas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada politica de firewall poderá ter uma configuração diferentes de IPS, sendo essas politicas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

6 ANÁLISE DE MALWARES MODERNOS

6.1 Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
6.2 O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
6.3 Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
6.4 Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;
6.5 Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
6.6 Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);
6.7 Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
6.8 A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

6.9 Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;

6.10 O sistema de análise "In Cloud" ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

6.11 O sistema automático de analise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

6.12 Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

6.13 Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

6.14 Deve permitir visualizar os resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

6.15 Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso positivo e falso-negativo na análise de malwares de dia Zero a partir da própria interface de gerência;

6.16 Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

6.17 Caso seja necessárias licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

6.18 Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado.

7 FILTRO DE URL

7.1 A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

7.1.1 Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

7.1.2 Deve ser possível a criação de politicas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança;

7.1.3 Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

7.1.4 Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

7.1.5 Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;
7.1.6 Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;
7.1.7 Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;
7.1.8 Possui pelo menos 60 categorias de URLs;
7.1.9 A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;
7.1.10 Suporta a criação categorias de URLs customizadas;
7.1.11 Suporta a exclusão de URLs do bloqueio, por categoria;
7.1.12 Permite a customização de página de bloqueio;
7.1.13 Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);
7.1.14 A funcionalidade de Filtro de URL deve operar em caráter permanente, para base ou cache instalado na solução até a data de vencimento da licença, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante;
7.1.15 Suporta a inclusão nos logs do produto de informações das atividades dos usuários;
7.1.16 Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For.

8 IDENTIFICAÇÃO DE USUÁRIOS

8.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;
8.2 Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
8.3 Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;
8.4 Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

8.5 Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em Usuários e Grupos de usuários;

8.6 Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;

8.7 Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

8.8 Suporte a autenticação Kerberos;

8.9 Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive Portal e usuário de VPN SSL;

8.10 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

8.11 Deve identificar usuários através de leitura do campo x-fowarded-for, populando nos logs do firewall o endereço IP, bem como o usuário de rede responsável pelo acesso;

8.12 Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;

8.13 Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

8.14 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores Windows.

9 QOS

9.1 Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

9.2 Suportar a criação de políticas de QoS por:

9.2.1 Endereço de origem;

9.2.2 Endereço de destino;

9.2.3 Por usuário e grupo do LDAP/AD;

9.2.4 Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

9.2.5 Por porta;

9.3 O QoS deve possibilitar a definição de classes por:

9.3.1 Banda Garantida;

9.3.2 Banda Máxima;
9.3.3 Fila de Prioridade.

9.4 Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

9.5 Suportar marcação de pacotes Diffserv, inclusive por aplicação;

9.6 Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);

9.7 Disponibilizar estatísticas RealTime para classes de QoS;

9.8 Deve suportar QOS (traffic-shapping), em interface agregadas;

9.9 Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

10 FILTRO DE DADOS

10.1 Permite a criação de filtros para arquivos e dados pré-definidos;

10.2 Os arquivos devem ser identificados por extensão e assinaturas;

10.3 Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);

10.4 Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;

10.5 Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;

10.6 Permitir listar o número de aplicações suportadas para controle de dados;

10.7 Permitir listar o número de tipos de arquivos suportados para controle de dados;

11 Geo-localização

11.1 Suportar a criação de politicas por Geo Localização, permitindo o trafego de determinado Pais/Países sejam bloqueados.

11.2 Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

11.3 Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar politicas utilizando as mesmas.

12 VPN

12.1 Suportar VPN Site-to-Site e Cliente-To-Site;

12.2 Suportar IPSec VPN;

12.3 Suportar SSL VPN;

12.4 A VPN IPSEc deve suportar:

12.4.1 DES e 3DES;
12.4.2 Autenticação MD5 e SHA-1;

12.4.3 Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
12.4.4 Algoritmo Internet Key Exchange (IKEv1 e v2);
12.4.5 AES 128, 192 e 256 (Advanced Encryption Standard)
12.4.6 Autenticação via certificado IKE PKI.

12.5 Deve possuir interoperabilidade com os seguintes fabricantes:
12.5.1 Cisco;
12.5.2 Checkpoint;
12.5.3 Juniper;
12.5.4 Palo Alto Networks;
12.5.5 Fortinet;
12.5.6 Sonic Wall;

12.6 Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de troubleshooting;

12.7 A VPN SSL deve suportar:
12.7.1 O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
12.7.2 A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
12.7.3 Atribuição de endereço IP nos clientes remotos de VPN SSL;
12.7.4 Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
12.7.5 Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
12.7.6 Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
12.7.7 Atribuição de DNS nos clientes remotos de VPN;
12.7.8 Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac, Windows e Chrome OS);
12.7.9 A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;
12.7.10 Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;
12.7.11 Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
12.7.12 Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

12.7.13 Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;
12.7.14 Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
12.7.15 A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
12.7.16 Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;
12.7.17 Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;
12.7.18 Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;
12.7.19 Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
12.7.20 Suporta leitura e verificação de CRL (certificate revocation list);
12.7.21 Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
12.7.22 O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;
12.7.23 O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário;
12.7.24 Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:
12.7.24.1 Antes do usuário autenticar na estação;
12.7.24.2 Após autenticação do usuário na estação;
12.7.24.3 Sob demanda do usuário;
12.7.25 Deverá manter uma conexão segura com o portal durante a sessão.
12.7.26 O agente de VPN SSL client-to-site deve ser compatível com pelo menos:
12.7.26.1 Windows XP, Vista Windows 7, Windows 8, Mac OSx e Chrome OS;
12.7.27 O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;
12.7.28 Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;
12.7.29 Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna.

13 CONSOLE DE GERÊNCIA E MONITORAÇÃO

13.1 Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;

13.2 O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

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

13.4 O gerenciamento deve permitir/possuir:

- 13.4.1 Criação e administração de políticas de firewall e controle de aplicação;
- 13.4.2 Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 13.4.3 Criação e administração de políticas de Filtro de URL;
- 13.4.4 Monitoração de logs;
- 13.4.5 Ferramentas de investigação de logs;
- 13.4.6 Debugging;
- 13.4.7 Captura de pacotes.

13.5 Acesso concorrente de administradores;

13.6 Deve mostrar ao administrador do firewall a hora e data do último login e tentativas de login com falha para acessos a partir da interface gráfica e CLI.

13.7 Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso dos mesmo na configuração do dispositivo;

13.8 Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

13.9 Deve permitir usar palavras chaves e cores para facilitar identificação de regras;

13.10 Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;

13.11 Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;

13.12 Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;

13.13 Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

13.14 Autenticação integrada ao Microsoft Active Directory e servidor Radius;

13.15 Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;

13.16 Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

13.17 Criação de regras que fiquem ativas em horário definido;

13.18 Cri ação de regras com data de expiração;

13.19 Backup das configurações e rollback de configuração para a última configuração salva;
13.20 Suportar Rollback de Sistema Operacional para a ultima versão local;
13.21 Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
13.22 Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
13.23 Validação de regras antes da aplicação;
13.24 Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
13.24.1 É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
13.25 Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
13.25.1 É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
13.26 Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
13.27 Deve possibilitar a integração com outras soluções de SIEM de mercado (thirdparty SIEM vendors).
13.28 Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
13.29 Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
13.30 Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
13.31 Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS,Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
13.32 Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;
13.33 O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
13.34 Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.
13.35 Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;

13.36 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;
13.37 Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;
13.38 Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
13.39 Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
13.40 Deve ser possível exportar os logs em CSV;
13.41 Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.
13.42 Rotação do log;
13.43 Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
13.44 Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
  13.44.1 Situação do dispositivo e do cluster;
  13.44.2 Principais aplicações;
  13.44.3 Principais aplicações por risco;
  13.44.4 Administradores autenticados na gerência da plataforma de segurança;
  13.44.5 Número de sessões simultâneas;
  13.44.6 Status das interfaces;
  13.44.7 Uso de CPU.
13.45 Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
  13.45.1 Resumo gráfico de aplicações utilizadas;
  13.45.2 Principais aplicações por utilização de largura de banda de entrada e saída;
  13.45.3 Principais aplicações por taxa de transferência de bytes;
  13.45.4 Principais hosts por número de ameaças identificadas;
  13.45.5 Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;
  13.45.6 Deve permitir a criação de relatórios personalizados;
13.46 Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP’s distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;
13.47 Gerar alertas automáticos via:
  13.47.1 Email;
  13.47.2 SNMP;

13.47.3 Syslog.

13.48 A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

ESTADO DO CEARÁ

PODER JUDICIÁRIO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA – TR

ANEXO II – GARANTIA E SUPORTE TÉCNICO

1 A solução fornecida deverá estar coberta por garantia, compreendendo os defeitos decorrentes de projeto, fabricação, construção ou montagem, pelo período mínimo especificado individualmente em cada item, a contar da data de emissão da nota fiscal;

2 Durante o período de garantia, deve ser possível realizar a atualização de software (firmware) dos equipamentos para resolução de problemas de software (correção de bugs);

3 A garantia deve incluir envio de peças/equipamentos de reposição nos locais especificados contratualmente;

4 Os chamados serão abertos diretamente com a empresa fornecedora da solução através de ligação telefônica, website e/ou email. O suporte da empresa fornecedora da solução deverá operar de segunda a sexta-feira, das 8 às 18 horas. O atendimento inicial deverá ocorrer em até 4 horas úteis;

5 A empresa fornecedora da solução deverá disponibilizar um portal web 24x7 com sistema de help-desk para abertura de chamados de suporte técnico. Mediante login e senha de acesso ao sistema, os membros da equipe técnica da contratante poderão abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico;

6 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

7 A empresa fornecedora da solução deverá prestar o suporte de primeiro nível e caso julgue necessário poderá escalar o suporte ao fabricante dos equipamentos, ficando a empresa fornecedora da solução responsável por gerenciar o chamado durante todo o tempo em que o mesmo permanecer aberto;

8 A empresa fornecedora da solução poderá recorrer ao suporte do fabricante quando se tratarem de correções especiais, defeitos nos programas (firmwares) ou defeitos em hardwares que necessitem de reparos especiais, correções de bugs ou substituições de peças e/ou equipamentos;

9 Detectada a necessidade de substituição de peças/equipamentos, o envio do substituto deverá ocorrer em até 30 (trinta) dias úteis ou conforme especificado individualmente em cada item (prevalecendo o de menor prazo menor). A empresa fornecedora da solução deverá arcar com os custos do deslocamento do envio da peça de substituição, ficando a contratante responsável pelo envio da peça defeituosa;

10 Deve ser possível o contato direto da contratante com o fabricante dos equipamentos em horários não compreendidos pelos suportes da empresa fornecedora da solução, ou quando a contratante julgar necessário. O suporte do fabricante dos equipamentos deve operar em regime 24x7 (24 horas por dia, 7 dias por semana), com atendimento através de ligação telefônica para atendimentos emergenciais;

11 Não serão aceitos suportes compartilhados para envio de peças de reposição (shared support);

12 A empresa deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico, cabendo a este órgão a abertura do chamado com intermediação da empresa fornecedora dos equipamentos ou diretamente com o fabricante dos equipamentos.

13 Os serviços de suporte técnico remoto deverá atender as seguintes premissas:

13.1 A empresa fornecedora da solução deverá disponibilizar, cumulativamente, estrutura de suporte técnico por meio de atendimento telefônico, website e e-mail;

13.2 As ligações deverão ser gratuitas, adotando-se o sistema 0800;

13.3 A empresa fornecedora da solução deverá disponibilizar um portal web com disponibilidade de 24 horas por dia, 7 dias por semana e 365 dias por ano, com sistema de help-desk para abertura de chamados de suporte técnico;

13.4 A equipe técnica da contratante poderá abrir, gerenciar status e conferir todo o histórico de chamados de suporte técnico, mediante login e senha de acesso ao sistema;

13.5 Os chamados abertos por e-mail deverão ter sua abertura automática no portal web;

13.6 Todo o chamado aberto deverá ter sua resolução técnica registrada no sistema web de help-desk;

13.7 A empresa fornecedora da solução deverá prestar o suporte técnico dos produtos, sendo facultado a ela o escalonamento das questões para o respectivo fabricante, ficando, entretanto, a empresa fornecedora da solução responsável pelo gerenciamento do chamado e prestação de informações à contratante;

13.8 A empresa fornecedora da solução deve indicar, por ocasião do início dos trabalhos, os procedimentos para abertura de suporte técnico.

13.9 A empresa fornecedora da solução deverá alocar até 4 horas mensais, no máximo, durante o intervalo de garantia do equipamento, sem custo adicional, não cumulativo e vedada ultrapassar esse intervalo, para atendimento remoto de demandas de manutenção, conforme necessidade da Contratante. Chamados técnicos da garantia dos produtos não estão compreendidos neste intervalo mensal.

13.10 As horas de atendimento serão realizadas normalmente em horário comercial, no período compreendido entre 08:30 e 18:30h, em dias de semana (segunda à sexta);

13.11 Horas que porventura precisem ser realizadas fora do horário comercial serão contabilizadas de acordo com a tabela:

Horário de Trabalho	**Contabilização de horas (fator de conversão)**
Entre 08:30 e 18:30 (dias de semana, segunda à sexta)	Cada hora trabalhada equivale a 1h
Entre 18:31 e 08:29 (dias de semana, segunda à sexta)	Cada hora trabalhada equivale a 1,5h
Em finais de semana (sábados e domingos)	Cada hora trabalhada equivale a 2h
Em feriados nacionais, estaduais e municipais	Cada hora trabalhada equivale a 2h

14 Prestação de serviços que compreendem, entre outros, os seguintes procedimentos de serviços da Solução de Plataforma de Segurança:

14.1 Alteração de qualquer configuração de topologia que esta Corte julgue necessário;
14.2 Habilitar licenças que porventura sejam adquiridas;
14.3 Sanar dúvidas relacionadas ao funcionamento dos equipamentos;
14.4 Administração e configuração da Solução de Gerenciamento Centralizado de firewall;
14.5 Suporte em caso de indisponibilidade de links e interfaces do cluster de firewall;
14.6 Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários desta Corte que dependam do cluster de firewall;
14.7 Suporte à configuração e resolução de problemas de acessos remotos VPNs client-to-site;
14.8 Suporta à configuração e resolução de problemas de VPNs site-to-site entre o cluster de firewall e outros equipamentos quando solicitado;
14.9 Suporte quanto a problemas de identificação de usuários;
14.10 Suporte quanto a de problemas de desconexão de aplicações;
14.11 Auxilio quanto as atualizações de sistema operacional e assinaturas de aplicação, prevenção de ameaças e filtro de URL;
14.12 Configurações e resolução de problemas quanto a funcionalidades aplicação, prevenção de ameaças e filtro de URL;
14.13 Realizar alterações de regras de roteamento estático, roteamento dinâmico (OSPF e BGP), PBF (Policy Base Routing) e tipos de NAT quando solicitado;
14.14 Realizar liberações ou bloqueios de aplicações quando solicitado;
14.15 Auxílio na customização de relatórios disponíveis na solução;
14.16 Verificação de funcionamento de regras;
14.17 Suporte na configuração de de-criptografia HTTPs inbound e outbound;
14.18 Auxílio na configuração de contextos virtuais;
14.19 Realizar manutenções preventivas do cluster de firewall quando solicitado;
14.20 Suporte em demais configurações de segurança, redundância e gerência;
14.21 Realizar otimização de performance (“tunning”) da solução de firewall;
14.22 Apoio técnico em configurações de alta disponibilidade, redundância e gerência de controladoras e pontos de acesso;
14.23 Suporte, administração e monitoramento das políticas e tarefas de backup;
14.24 Apoio técnico para tarefas de auditoria e análise de logs;
14.25 Encaminhar incidentes ao fabricante da solução;
14.26 Suporte técnico para identificação e resolução de problemas em software e hardware.

ESTADO DO CEARÁ

PODER JUDICIÁRIO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA – TR

ANEXO III – SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO e MIGRAÇÃO

1 A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço pode ser realizado remotamente através de webconferência ou videoconferência;

2 O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter o objetivo dos serviços, as atividades que serão realizadas, os prazos estimados para cada atividade, as diretrizes dos serviços que serão realizados, os locais de execução, as informações necessárias, os padrões que serão aplicados, o nome do(s) gerente(s) de projetos responsável e do(s) técnico(s) responsável(is) pela execução dos serviços. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

3 Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a empresa fornecedora da solução sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à contratante a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

4 Após a instalação deve ser monitorado pelo prazo mínimo de 24 horas corridas as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação;

5 Ao final da instalação, deverá ser realizado o repasse de informações hands-on, apresentando as configurações realizadas nos equipamentos, de no mínimo 2 (duas) horas, ou conforme disposto individualmente em cada item (prevalecendo o disposto em individualmente em cada item). A contratante disponibilizará o local adequado para a transferência do conhecimento e acesso aos equipamentos de produção;

6 Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante dos equipamentos. Em momento anterior à instalação, a contratante poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

7 Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso, configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

8 Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da contratante.

ESTADO DO CEARÁ

PODER JUDICIÁRIO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA – TR

ANEXO IV – MODELO DE TERMO DE CIÊNCIA

PJSETIN(AAAANNN) – (Nome do Projeto/Contratação, se for projeto)

INTRODUÇÃO
Visa obter o comprometimento formal dos empregados da contratada diretamente envolvidos no projeto sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

IDENTIFICAÇÃO			
Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes na Contratante.

CIÊNCIA
CONTRATADA – Funcionários

_____ **<Nome>** **Matrícula: <Matr.>**	_____ **<Nome>** **Matrícula: <Matr.>**
_____ **<Nome>** **Matrícula: <Matr.>**	_____ **<Nome>** **Matrícula: <Matr.>**
_____ **<Nome>** **Matrícula: <Matr.>**	_____ **<Nome>** **Matrícula: <Matr.>**

_____,_____ de _____ de 20_____.

ESTADO DO CEARÁ
PODER JUDICIÁRIO
SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO
TERMO DE REFERÊNCIA – TR

ANEXO V – MODELO DE TERMO DE COMPROMISSO

PJSETIN(AAAANNN) – (Nome do Projeto/Contratação, se for projeto)

O *<NOME DO ÓRGÃO>*, sediado em *<ENDEREÇO>*, CNPJ n° *<CNPJ>*, doravante denominado CONTRATANTE, e, de outro lado, a *<NOME DA EMPRESA>*, sediada em *<ENDEREÇO>*, CNPJ n° *<CNPJ>*, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as

atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES.

Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem

como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro da <CIDADE DA CONTRATANTE>, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

CONTRATANTE	**CONTRATADA**
_____ *<Nome>* Matrícula: *<Matr.>*	_____ *<Nome>* *<Qualificação>*
Testemunhas	
Testemunha 1 _____ *<Nome>* *<Qualificação>*	**Testemunha 2** _____ *<Nome>* *<Qualificação>*

_____, _____ de _____ de 20____