PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ATA DE REGISTROS DE PREÇOS N. 013/2017 – CJF

PROCESSO N. CJF-ADM-2017/00046

PREGÃO ELETRÔNICO N 24/2017 - CJF

DADOS DA EMPRESA	
EMPRESA: NCT INFORMÁTICA LTDA	
CNPJ/MF: 03.017.428/0001-35	
ENDEREÇO: SBS, Quadra 02, Lote 03, Bloco Q, 8º Andar, Sala 801, Centro Empresarial João Carlos Saad, Brasília – DF, CEP: 70.070-120	
TELEFONE: (61) 3201-0000 (61) 98171.7647	**Contato:** Ana Paula
E-MAIL: Ana.Carvalho@nct.com.br; operacoes@nct.com.br;	
SIGNATÁRIO EMPRESA: PRISCILA KIN YAMAMOTO JORANHEZON – Sócia-Administradora	
SIGNATÁRIO CJF: Juiz Federal CLEBERSON JOSÉ ROCHA, Secretário-Geral respondendo pela Diretoria-Geral	

DADOS DA ATA
OBJETO: Registro de preço para contratação de solução para o gerenciamento de ameaças de segurança, contemplando o fornecimento de equipamentos, softwares e sistemas de gerenciamento da solução, com garantia de 60 meses e serviços de instalação e configuração, transferência de conhecimento e suporte técnico.
FUNDAMENTAÇÃO LEGAL: Lei n. 10.520/2002, Decreto n. 5.450/2005, Decreto n. 7.892/2013, e legislação correlata, aplicando-se, subsidiariamente, no que couberem, a Lei Complementar n. 123/2006 e alterações, regulamentada pelo Decreto n. 8.538/2015, Lei n. 8.666/1993 e alterações, e a Lei n. 12.846/2013 e, em conformidade com as informações constantes, no Processo n. CJF-ADM-2017/00046.
VIGÊNCIA: 28/12/2017 a 27/12/2018
VALOR DA ATA: R$ 4.521.400,00
UNIDADE FISCALIZADORA: STI
OBSERVAÇÕES: a) Vigência 12 meses a partir da assinatura.

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ATA DE REGISTRO DE PREÇOS N. 013/2017 - CJF

ÓRGÃO GERENCIADOR: **UNIÃO,** por intermédio do **CONSELHO DA JUSTIÇA FEDERAL**, Órgão integrante do Poder Judiciário, CNPJ/MF n. 00.508.903/0001-88, com sede no Setor de Clubes Esportivos Sul, Trecho III, Polo 8, Lote 9, Brasília-DF, neste ato representado pelo Secretário-Geral, respondendo pela Diretoria-Geral, o Juiz Federal **CLEBERSON JOSÉ ROCHA**, brasileiro, CPF/MF n. 654.729.346-72, Carteira de Identidade n. 1.872.124 - SSP/DF, residente em Brasília - DF.

DETENTORA: **NCT INFORMÁTICA LTDA**, pessoa jurídica de direito privado, CNPJ/MF n. 03.017.428/0001-35, com sede no SBS, Quadra 02, Lote 03, Bloco Q, 8º Andar, Sala 801, Centro Empresarial João Carlos Saad, Brasília – DF, CEP: 70.070-120, neste ato representada pela Sócia-Administradora, a Senhora **PRISCILA KIN YAMAMOTO JORANHEZON,** brasileira, CPF n. 022.373.811-51, Passaporte n. F109908 e Carteira de Identidade n. 2.373.366 – SSP/DF, residente em Brasília – DF.

As partes firmam, com fundamento na Lei n. 10.520, de 17 de julho de 2002, no Decreto n. 5.450, de 31 de maio de 2005, no Decreto n. 7.892, de 23 de janeiro de 2013, e legislação correlata, aplicando-se, subsidiariamente, no que couberem, a Lei Complementar n. 123, de 14 de dezembro de 2006 e alterações, regulamentada pelo Decreto n. 8.538, de 6 de outubro de 2015, a Lei n. 8.666, de 21 de junho de 1993 e alterações, e a Lei n. 12.846, de 1º de agosto de 2013 e, em conformidade com as informações constantes do Processo n. CJF-ADM-2017/00046, a presente **Ata de Registro de Preços n. 013/2017 - CJF**, mediante as cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – DO OBJETO

1.1. Registro de preço para contratação de solução para o gerenciamento de ameaças de segurança, contemplando o fornecimento de equipamentos, softwares e sistemas de gerenciamento da solução, com garantia de 60 meses e serviços de instalação e configuração, transferência de conhecimento e suporte técnico.

1.2. A existência de preço registrado não obriga o CJF a adquirir o objeto que dele poderá advir, sem que caiba direito de indenização à DETENTORA de qualquer espécie.

1.3. As disposições constantes no edital do Pregão Eletrônico n. 24/2017 e os atos subsequentes com ele relacionados integram o presente instrumento para todos os efeitos.

CLÁSULA SEGUNDA – DOS PREÇOS REGISTRADOS

2.1. **DOS PREÇOS REGISTRADOS** – O preço para o fornecimento dos produtos, serão praticados pela DETENTORA conforme descrito no Anexo IV – Planilha de Preços, desta Ata.

2.2. Os preços registrados serão fixos e irreajustáveis durante a vigência desta ata de registro de preços.

CLÁSULA TERCEIRA – DO CONTRATO

3.1. O Contrato será firmado com a DETENTORA da Ata de Registro de Preços com base na minuta constante do Módulo III do edital.

3.2. O prazo para assinatura do Contrato será de 05 (cinco) dias úteis, após regular convocação pelo ÓRGÃO GERENCIADOR, sujeitando-se, em caso de inadimplemento, às penalidades legais e as estabelecidas nesta Ata.

3.3. A assinatura do Contrato será efetuada na Seção de Contratos, situada no Setor de Clubes Esportivos Sul – SCES, Trecho III Polo 8 Lote 9, Brasília/DF, CEP 70200-003.

3.4. Farão parte integrante do Contrato todos os elementos apresentados pela DETENTORA no Pregão Eletrônico n. 24/2017 que tenham servido de base para o julgamento, bem como as condições estabelecidas no edital e respectivos anexos.

CLÁSULA QUARTA – DAS OBRIGAÇÕES DA DETENTORA

4.1. A DETENTORA obriga-se ao cumprimento de todas as disposições constantes do Módulo I – Termo de Referência e demais anexos do edital e, ainda, a:

a) Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução de segurança de acordo com os prazos definidos no Anexo III - Cronograma, contados a partir da emissão de Ordem de Serviço - OS pelo ÓRGÃO GERENCIADOR;

b) Fornecer os equipamentos e softwares da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do ÓRGÃO GERENCIADOR, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração;

c) Entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até **45 (quarenta e cinco) dias**, a contar da data de emissão da ordem de serviço pelo ÓRGÃO GERENCIADOR;

d) Realizar a transferência de conhecimento conforme descrito no subitem 7.3 do Módulo I;

e) Prestar garantia e suporte técnico conforme descrito nos subitens 7.4 e 7.5, respectivamente, do Módulo I;

f) Não subcontratar, no todo ou em parte, o objeto desta ata sem prévia

anuência do ÓRGÃO GERENCIADOR;

g) Demais obrigações constantes do item 7 do Módulo I do edital;

h) Manter durante todo o período de vigência desta Ata de Registro de Preços as condições de habilitação e qualificação exigidas para a contratação, comprovando-as, a qualquer tempo, mediante solicitação do ÓRGÃO GERENCIADOR.

CLÁUSULA QUINTA – DAS OBRIGACÕES DO ÓRGÃO GERENCIADOR

5.1. O ÓRGÃO GERENCIADOR obriga-se ao cumprimento de todas as disposições constantes do Módulo I – Termo de Referência do edital e, ainda, a:

a) Acompanhar e fiscalizar a execução do objeto contratual.

b) Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual.

c) Informar à DETENTORA de atos que possam interferir direta ou indiretamente nos serviços prestados;

d) Comunicar qualquer anormalidade ocorrida na execução dos serviços pela DETENTORA;

e) Avaliar todos os serviços prestados pela DETENTORA;

f) Responsabilizar-se pelos pagamentos dos serviços prestados pela DETENTORA mediante a apresentação de nota fiscal;

g) Indicar os seus representantes para fins de contato e demais providências inerentes à execução desta Ata e do Contrato;

h) Permitir o acesso dos técnicos habilitados e identificados da DETENTORA às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do ÓRGÃO GERENCIADOR, inclusive aqueles referentes à identificação, trânsito e permanência em suas dependências.

CLÁUSULA SEXTA – DO REGISTRO DE PREÇOS

6.1. Após a homologação da licitação, o registro de preços observará, entre outras, as seguintes condições:

a) será incluído, nesta ata, o registro das empresas que aceitarem cotar os produtos/serviços com preços iguais ao da empresa vencedora na sequência da classificação do certame;

b) o preço registrado com indicação das empresas será divulgado no Portal de Compras do Governo Federal e ficará disponibilizado durante a vigência desta ata de registro de preços; e

c) a ordem de classificação das empresas registrados na ata deverá ser respeitada nas contratações

6.2. O registro a que se refere o caput tem por objetivo a formação de cadastro de reserva, no caso de exclusão da primeira colocado desta ata, nas hipóteses previstas nos artigos 20 e 21, do Decreto n. 7.892/2013.

6.3. Serão registrados nesta ata de registro de preços, nesta ordem:

a) O preço e quantitativo da empresa mais bem classificado durante a etapa competitiva; e

b) O preço e quantitativo das empresas que tiverem aceitado cotar seus produtos em valor igual ao da empresa mais bem classificada.

6.4. Se houver mais de uma empresa na situação de que trata a alínea "b" acima, serão classificados segundo a ordem da última proposta apresentada durante a fase competitiva.

CLÁUSULA SÉTIMA – DA FISCALIZAÇÃO

7.1. O ÓRGÃO GERENCIADOR designará servidor para acompanhar e fiscalizar a execução desta Ata, nos termos do art. 67 da Lei n. 8.666/1993.

7.2. O ÓRGÃO GERENCIADOR reserva-se ao direito de, sem restringir a plenitude da responsabilidade da DETENTORA, exercer a mais ampla e completa fiscalização sobre os fornecimentos/serviços contratados.

CLÁUSULA OITAVA – DO RECEBIMENTO DO OBJETO

8.1. A entrega dos equipamentos, softwares e acessórios da solução e a realização dos serviços previstos nesta contratação deverão ser realizados na sede do CONTRATANTE, situada no Setor de Clubes Esportivos Sul - SCES - Trecho III, Polo 8, Lote 9, CEP 70200-003, Brasília/DF.

8.2. Será emitido Termo de Recebimento Provisório (TRP) após a entrega dos equipamentos, softwares, acessórios, plano de implantação e demais documentações da solução, conforme descrito no Anexo III – Cronograma.

8.3. A finalização da entrega deverá ser formalizada mediante comunicação escrita da DETENTORA ao ÓRGÃO GERENCIADOR. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da detentora, desde que não haja pendências a cargo da mesma.

8.4. A DETENTORA deverá concluir no prazo de 15 (quinze) dias corridos, contados a partir da emissão do termo de recebimento provisório, os serviços de instalação e configuração dos equipamentos e softwares da solução integrada de segurança, realizando todas as atividades programadas para esta etapa.

8.5. Será emitido Termo de Recebimento Definitivo (TRD), após a formalização por escrito da DETENTORA referente à conclusão das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança. O recebimento definitivo realizar-se-á no prazo máximo de 10 (dez) dias corridos, contados da comunicação da detentora, desde que não haja pendências a cargo da mesma.

8.6. Após a emissão do Termo de Recebimento Definitivo (TRD), a detentora deverá realizar, por 15 (quinze) dias corridos, operação assistida ON-SITE da solução de segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução.

8.6.1. O período de operação assistida ON-SITE da solução de segurança deverá ser executado presencialmente nas instalações do ÓRGÃO GERENCIADOR, 3 (três) horas por dia, no período entre 14h e 21h.

8.6.2. O período de operação assistida ON-SITE faz parte dos serviços de instalação e configuração, não representando ônus adicional para o ÓRGÃO GERENCIADOR.

CLÁUSULA NONA – DO PAGAMENTO

9.1. O pagamento será efetuado no prazo de 10 (dez) dias úteis, a contar da data do recebimento da nota fiscal e de acordo com os preços registrados, obedecendo ao disposto na Cláusula Décima Primeira do contrato.

CLÁUSULA DÉCIMA – DA VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

10.1. A presente Ata tem validade de 12 (doze) meses, a partir da data de assinatura.

CLÁUSULA DÉCIMA PRIMEIRA – DAS PENALIDADES

11.1. A DETENTORA, em caso de inadimplência, e observado o regular procedimento administrativo, assegurado o contraditório e a ampla defesa, nos termos da lei, ficará sujeita, isolada ou cumulativamente, às seguintes penalidades, sem prejuízo das demais previsões legais:

11.2. **Advertência**: sempre que forem observadas irregularidades de pequena monta para as quais tenha concorrido.

11.3. **Multa Moratória:** de 0,5% (cinco décimos por cento) por dia de atraso, calculada sobre o valor adjudicado na hipótese de atraso injustificado para a assinatura desta Ata.

11.4. **Multa Compensatória:** de 10% (dez por cento) sobre o valor da nota de empenho quando superado o prazo de 30 (trinta) dias estabelecido no subitem 11.3 desta cláusula ou considerada desistente.

1.5. **Impedimento de Licitar e Contratar:** com a União, pelo prazo de até 5 (cinco) anos, nos termos do art. 7º da Lei n. 10.520/2002 c/c o art. 28 do Decreto n. 5.450/2005.

11.6. **Suspensão Temporária:** pela inexecução total ou parcial do objeto, será suspensa temporariamente de participar de licitação e impedimento de contratar a Administração, por prazo não superior a 2 (dois) anos, nos termos do inciso III, artigo 87 da Lei n. 8.666/1993, conforme Acordão 2242/2013, do Plenário do Tribunal de Contas da União.

11.7. **Declaração de Inidoneidade:** ser declarada inidônea, nos termos do inciso IV do art. 87 da Lei n. 8.666/1993.

11.8. As multas previstas nos subitens 11.2 e 11.4 poderão cumular-se entre si, bem como com as penalidades dos subitens 11.2, 11.5 e 11.7.

11.9. Nos termos do §3º do art. 86 e do §1º do art. 87 da Lei n. 8.666/1993, a multa, caso aplicada após regular processo administrativo, será descontada do pagamento eventualmente devido ao órgão gerenciador ou ser recolhida ao Tesouro por GRU (Guia de Recolhimento da União) no prazo máximo de 5 (cinco) dias úteis, contados da notificação ou, ainda, quando for o caso, cobrada judicialmente, em conformidade com a legislação específica.

11.10. A aplicação das sanções previstas nesta cláusula será feita mediante procedimento administrativo específico. O órgão gerenciador comunicará à DETENTORA sua intenção de aplicação da penalidade, assegurando-lhe o direito ao contraditório e à defesa prévia, no prazo de 5 (cinco) dias úteis, contados a partir do recebimento da comunicação.

11.11. Decidida pelo órgão gerenciador a aplicação de sanção, fica assegurado à Detentora o uso dos recursos previstos em lei. As sanções serão registradas no Sistema de Cadastramento Unificado de Fornecedores-SICAF.

11.12. Após assinatura da ata, em caso de inadimplência, a detentora sujeitar-se-á às penalidades nela previstas.

CLÁUSULA DÉCIMA SEGUNDA – DO CANCELAMENTO DO REGISTRO DE PREÇOS

12.1. A DETENTORA terá seu registro cancelado quando:

12.2. Ocorrer uma ou mais hipóteses previstas nos artigos 20 e 21 do Decreto n. 7.892/2013.

12.3. Ocorrer alguma das hipóteses contidas no art. 78 e seus incisos da Lei n. 8.666/1993.

CLÁUSULA DÉCIMA TERCEIRA – DAS DISPOSIÇÕES GERAIS

13.1. O compromisso de fornecimento só estará caracterizado mediante assinatura desta Ata de Registro de Preços e contrato.

13.2. O registro de preços será obrigatoriamente utilizado pelo órgão gerenciador, salvo quando a contratação se revelar antieconômica ou quando houver necessidade específica de outra forma de aquisição, devidamente justificada, hipótese, esta, em que será assegurada à DETENTORA a preferência, em igualdade de condições, nos termos do art. 16 do Decreto n. 7.892/2013.

13.3. Nos termos do §1º do art. 12 do Decreto 7.892/2013 é vedado efetuar acréscimos nos quantitativos fixados pela ata de registro de preços.

13.4. O quantitativo decorrente das adesões à Ata de Registro de Preços não poderá exceder, na totalidade, ao quíntuplo do quantitativo de cada item registrado para o

ÓRGÃO GERENCIADOR e órgãos participantes, independentemente do número de órgãos não participantes que aderirem, conforme definido no §4º do art. 22 do Decreto n. 7.892/2013.

CLÁUSULA DÉCIMA QUARTA – DO FORO

14.1. O Foro Juízo Federal da Seção Judiciária do Distrito Federal é competente para dirimir qualquer dúvida oriunda desta ata de registro de preços, com renúncia expressa a qualquer outro que as partes tenham ou venham a ter, por privilegiado ou especial que seja.

Brasília – DF, 28 de dezembro de 2017.

Juiz Federal CLEBERSON JOSÉ ROCHA
Secretário-Geral, respondendo pela
Diretoria-Geral do Conselho da Justiça Federal

PRISCILA KIN YAMAMOTO JORANHEZON
Sócia-Administradora da empresa
NCT Informática Ltda

PODER JUDICIÁRIO
CONSELHO DA JUSTIÇA FEDERAL

ATA DE REGISTRO DE PREÇOS N. 013/2017 – CJF

MÓDULO I – TERMO DE REFERÊNCIA

1. OBJETO

Registro de preços para contratação de solução para o gerenciamento de ameaças de segurança, contemplando o fornecimento de equipamentos, softwares e sistemas de gerenciamento da solução, com garantia de 60 meses e serviços de instalação e configuração, transferência de conhecimento e suporte técnico, para atendimento das necessidades do Conselho da Justiça Federal - CJF, de acordo com as especificações técnicas contidas no Termo de Referência.

2. JUSTIFICATIVA

Em 2013 o CJF realizou a contratação de solução integrada de segurança, compreendendo o fornecimento de solução de gerenciamento unificado de ameaças, firewall de aplicação web, que incluía a solução para armazenamento de logs destes produtos, bem como solução para o gerenciamento de vulnerabilidades de segurança, além dos serviços de instalação e garantia pelo período de 48 meses. Tendo sido assinado o termo de recebimento definitivo CJF-TRM-2014/00074 em 31 de janeiro de 2014. Tendo em vista a natureza contínua da prestação dos serviços, e as limitações determinadas pelo inciso II do Art. 57 da lei 8.666/93, torna-se necessária nova contratação para execução a partir de 01 de fevereiro de 2018.

Durante a fase de levantamento de viabilidades, levantou-se a possibilidade de manter-se a solução atual, estendendo-a para cobrir as novas necessidades descritas acima. No entanto, dada a existência de outros fabricantes no mercado que podem igualmente oferecer a proteção requerida pela organização, o que afasta a hipótese de inexigibilidade de licitação existente no artigo 25 da lei 8.666/93, obriga a Administração a licitar nova solução.

Justifica-se esta contratação pela necessidade que este Conselho tem, de prestação continuada de serviços de segurança capazes de regular o tráfego entre as distintas redes internas da Secretaria do Conselho bem como entre este e os Tribunais Regionais Federais, impedir a transmissão e recepção de tráfego nocivo, implementar recursos de criptografia para tunelamento em redes inseguras de comunicação (VPN), identificar, prevenir e bloquear tentativas de intrusão, realizar serviços de filtro de conteúdo web, monitorar e regular as solicitações feitas a aplicações web, fazer a gestão das vulnerabilidades encontradas em sistemas e recursos de TI e monitorar eventos que possam afetar a segurança computacional da instituição.

Porém, observaram-se avanços na tecnologia utilizada por malfeitores que não podiam ser previstas a época da confecção do termo de referência da última contratação, e para qual os produtos fornecidos não fornecem proteção adequada a este Conselho. Destes pode-se salientar os ataques de "dia zero", nome utilizado na indústria de segurança da informação para ataques utilizados por meio da exploração de uma vulnerabilidade anteriormente desconhecida que afeta de maneira adversa programas, dados, computadores e redes. Códigos maliciosos que exploram tais vulnerabilidades não podem ser detectados pelo método tradicional de assinatura utilizado pela solução ora em uso. Desta forma, são necessárias outras formas de detecção, como o uso de métodos heurísticos de análise, emulação de código e virtualização.

Um propósito malicioso também inexistente quando da aquisição da contratação anterior são as Ameaças Avançadas Persistentes, ou APT (Advanced Persistent Threat). Podem ser definidos como um conjunto de processos furtivos e contínuos de exploração de vulnerabilidades computacionais e engenharia social tendo como alvo uma entidade específica, por meio de técnicas sofisticadas. Apesar das atividades de um APT serem, por natureza, dissimuladas e de difícil detecção, o tráfego de rede de comando e controle associado é passível de detecção em nível de camada de rede, motivo pelo qual tais características foram requeridas neste Termo. Não obstante o valor agregado ao uso de tecnologias de gerenciamento de eventos e segurança de informação (SIEM – Security Information and Event Management) na análise em tempo real de alertas de segurança gerados pelo hardware de rede, segurança e aplicações, optou-se pela não inclusão de componente de SIEM na presente solução pela inerente complexidade em sua aquisição, implementação e uso, bem como a relativa falta de maturidade e de pessoal especializado na organização que viabilizasse seu eficaz uso.

Ademais, observa-se a necessidade de análise de segurança do tráfego "leste-oeste" como medida para evitar técnicas de exploração lateral, onde um criminoso cibernético consegue acesso a uma máquina de usuário ou a um servidor de rede com serviços pouco relevantes e utiliza este ponto de acesso para procurar dentro de seu segmento

de rede, sem passar pelos dispositivos de segurança de perímetro, outros serviços mais críticos para atacar. Uma forma de remediação deste tipo de ataque é a análise de todo o tráfego em nível de host, por meio da integração com o produto de infraestrutura virtual de servidores – Vmware, assim foi especificada solução que permite a análise anti-malware deste ambiente.

A proposta deste projeto é a substituição dos atuais equipamentos que compõem a solução de segurança por uma nova solução ou a manutenção da solução de gerenciamento de ameaças (UTM), atualmente em uso, com a adição de novas funcionalidades em face das novas tecnologias que trarão benefícios ao Conselho, tais como: elevar a capacidade de prevenção de ataques, permitir a avaliação das vulnerabilidades a que os ativos de TI estão sujeitas, possibilitando a eliminação antes que sejam exploradas, permitir a monitoração e que permita proteger as chamadas de sistema a aplicações disponibilizadas em servidores web, mesmo criptografadas, a análise avançada de ameaças evasivas e persistentes e análise de tráfego de rede dentro do ambiente de servidores, não apenas no perímetro com as redes externas e com a internet.

Assim, o presente Termo de Referência objetiva a aquisição de solução de segurança, contemplando o fornecimento de equipamentos, softwares e sistemas de gerenciamento da solução, com garantia de 60 meses e serviços de instalação e configuração, transferência de conhecimento e suporte técnico, de acordo com as especificações técnicas contidas no Termo de Referência, para atendimento das necessidades do Conselho da Justiça Federal.

A contratação utilizará o SISTEMA DE REGISTRO DE PREÇO (SRP) pois a solução será adquirida sob demanda, ou seja, uma quantidade inicial de licenças e equipamentos serão solicitados visando a manutenção operacional dos serviços de segurança que atualmente protegem o CJF e novos serviços e produtos de segurança poderão ser solicitados ao longo da vigência da Ata de Registro de Preços, incrementando a capacidade de proteção do ambiente tecnológico, conforme a disponibilidade orçamentária do CJF. A previsão de entregas parceladas do objeto, em virtude da impossibilidade de se definir previamente o quantitativo a ser demandado pela Administração, está prevista no Decreto N° 7.892/2013, Art. 3°, inciso II e IV.

3. DESCRIÇÃO DOS PRODUTOS

3.1. Quadro demonstrativo dos produtos atualmente implantados no CJF:

PRODUTO	QUANTIDADE
UTM Bundle - equipamentos modelo FortiGate 1500D da FORTINET, em cluster.	01
WAF - equipamentos modelo FortiWeb 3000D da FORTINET, em cluster.	01
Centralizador de logs e relatórios - equipamento modelo FortiAnalyzer 2000B da FORTINET.	01
Gestão de vulnerabilidades – software Control Compliance Suite Vulnerability Manager Virtual Appliance (CCSVM) da SYMANTEC.	5000 ativos

3.2. O detalhamento do ambiente tecnológico do CJF está descrito no ANEXO II.

4. DO FORNECIMENTO

4.1. As soluções e serviços descritos neste Termo de Referência poderão ser fornecidos por:

4.1.1. Renovação e complementação de licenças e/ ou substituição dos equipamentos atualmente instalados no CONTRATANTE (subitem 3.1); ou

4.1.2. Substituição total das soluções de segurança atualmente implantada no CONTRATANTE (Item 3).

4.2. Independentemente das opções descritas acima, as soluções ofertadas devem atender integralmente as especificações técnicas deste Termo de Referência.

5. QUANTITATIVOS

5.1. O objeto da contratação é uma solução de segurança, composta por equipamentos e softwares com garantia por 60 meses, serviços de instalação e configuração, serviço de transferência de conhecimento e serviço de suporte técnico por 60 meses, contados a partir da emissão do Termo de Recebimento Definitivo.

5.2. O conjunto dos requisitos especificados para o LOTE 01 (itens 1, 2, 3, 4, 5) poderão ser atendidos por meio de um único equipamento ou pela composição dos equipamentos, produtos, peças e softwares que os compõem, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança.

Desta forma, abre-se para que o mercado defina qual a composição que melhor atende aos requisitos técnicos aqui descritos, tendo como baliza o menor custo global para a Administração.

LOTE	ITEM	DESCRIÇÃO	Qtd.
1	1	Solução em cluster de Gerenciamento Unificado de Ameaças (UTM).	01
	2	Solução de Prevenção contra-Ataques Avançados (APT).	01
	3	Solução de Armazenamento de Logs.	01
	4	Solução de Gerenciamento.	01
	5	Solução de Segurança Multifunção para Ambiente Virtualizado.	18 hosts (36 sockets)
	6	Serviço de Instalação e Configuração das Soluções.	01
	7	Serviço de Suporte Técnico (mensal).	60
	8	Transferência de Conhecimento (por pessoa).	02
2	1	Solução em cluster de Firewall de Aplicação Web (WAF).	01
	2	Serviço de Instalação e Configuração da Solução.	01
	3	Serviço de Suporte Técnico (mensal).	60
	4	Transferência de Conhecimento (por pessoa).	02
3	1	Solução de Gestão de Vulnerabilidades	01
	2	Serviço de Instalação e Configuração da Solução.	01
	3	Serviço de Suporte Técnico (mensal).	60
	4	Transferência de Conhecimento (por pessoa).	02

6. DA EXECUÇÃO DO OBJETO

6.1. A solução para o gerenciamento de ameaças de segurança deverá operar de forma integrada, ou seja, os equipamentos, softwares fornecidos e configurações aplicadas pela CONTRATADA deverão operar como um conjunto plenamente ajustado, de forma a garantir desempenho, disponibilidade e funcionalidades adequados aos requisitos do Conselho.

6.2. A solução para o gerenciamento de ameaças de segurança será composta por Lote 01: gerenciamento de ameaças, prevenção contra-ataques avançados, armazenamento de logs, gerenciamento e segurança multifunção para ambiente virtualizado; por Lote 02: firewall de aplicação web e por Lote 03: gestão de vulnerabilidades. Todos os softwares e sistemas de gerenciamento, necessários para seu completo funcionamento, que deverão ser integrados ao ambiente tecnológico do CJF (detalhado no ANEXO II).

6.3. Os modelos e versões dos equipamentos (hardware) que compõe a solução para o gerenciamento de ameaças de segurança deverão ser ofertados novos, sem uso anterior, e deverão permanecer em linha de produção pelos próximos 12 (doze) meses e suportar a última versão de sistema operacional do fabricante pelos próximos 5 (cinco) anos, contados da data da emissão do Termo de Recebimento Definitivo.

7. OBRIGAÇÕES DA CONTRATADA

7.1. Obrigações Gerais

7.1.1. Fornecer os equipamentos e softwares da solução com todos os itens acessórios necessários à sua perfeita instalação, funcionamento e integração ao ambiente computacional do CJF, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração.

7.1.2. Acatar as normas e diretrizes estabelecidas pelo CONTRATANTE para o fornecimento dos produtos e execução dos serviços objeto deste Termo de Referência.

7.1.3. Submeter à prévia aprovação da CONTRATANTE toda e qualquer alteração pretendida na prestação dos serviços.

7.1.4. Manter, durante a execução do contrato a ser firmado, as condições de habilitação e qualificação exigidas na licitação.

7.1.5. Sujeitar-se à fiscalização da CONTRATANTE, no tocante ao fornecimento e a prestação dos serviços, prestando todos os esclarecimentos solicitados e atendendo de imediato às reclamações fundamentadas, caso venham a ocorrer.

7.1.6. Prestar as atividades objeto da licitação, por meio de mão de obra especializada e devidamente certificada pelos fabricantes dos equipamentos e softwares que compõem a solução integrada de segurança.

7.1.7. Não utilizar pessoal técnico já alocado em contratos ou projetos em execução no CONTRATANTE para prestar as atividades objeto da licitação, devendo compor equipe exclusiva para este fim.

7.1.8. Credenciar devidamente um Representante Técnico para, em todas as questões relativas ao cumprimento do objeto, representar a CONTRATADA.

7.1.9. O profissional indicado atuará desde o início da execução do contrato até a conclusão da implantação como Gerente de Projeto, devendo possuir certificação PMP (Project Management Professional).

7.1.10. Propor os ajustes necessários à adequação, segurança e racionalização dos serviços prestados, respeitando o objeto deste Termo de Referência.

7.1.11. Responsabilizar-se por todos os ônus referentes aos serviços objeto deste Termo de Referência, inclusive salários de pessoal, alimentação, diárias, hospedagem, transporte e seguros, bem como tudo que as leis trabalhistas e previdenciárias preveem e demais exigências legais para o exercício da atividade objeto desta licitação.

7.1.12. Responsabilizar-se integralmente pela sua equipe técnica, primando pela qualidade, desempenho, eficiência e produtividade, visando à execução dos trabalhos durante todo o Contrato, dentro dos prazos estipulados, sob pena de ser considerada infração passível de aplicação das penalidades previstas, caso os prazos e condições não sejam cumpridas.

7.1.13. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de pagamentos adicionais ao CONTRATANTE ou a não prestação satisfatória dos serviços.

7.1.14. Guardar inteiro sigilo dos dados processados, reconhecendo serem estes de propriedade exclusiva do CONTRATANTE.

7.1.15. Substituir imediatamente, a critério do CONTRATANTE, a qualquer tempo, e sem nenhum ônus adicional, qualquer profissional do seu corpo técnico cuja presença seja considerada indesejável ou inconveniente, em virtude de comportamento inadequado.

7.1.16. Acatar, nas mesmas condições ofertadas, nos termos do art. 65, § 1º, da Lei nº 8.666/93, as solicitações da CONTRATANTE para acréscimos ou supressões que se fizerem necessárias à execução do objeto licitado.

7.1.17. Assumir a responsabilidade por danos causados diretamente à Administração ou a terceiros, decorrentes de sua culpa ou dolo na execução do objeto licitado, não excluindo ou reduzindo essa responsabilidade a fiscalização ou o acompanhamento pelo CONTRATANTE.

7.1.18. Sujeitar-se a mais ampla e irrestrita fiscalização, por parte da Equipe de Fiscalização e Recebimento indicada pelo CONTRATANTE para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e atendendo às reclamações formuladas.

7.1.19. Comunicar a Equipe de Fiscalização e Recebimento, por escrito, qualquer anormalidade que ponha em risco o fornecimento ou a execução dos serviços.

7.1.20. Corrigir as falhas detectadas pela Equipe de Fiscalização e Recebimento indicada pelo CONTRATANTE.

7.1.21. Executar as atividades previstas no contrato em estrito cumprimento aos prazos previstos no ANEXO III – Cronograma de Implantação.

7.2. **Quanto à entrega, instalação e configuração dos equipamentos e softwares da solução.**

7.2.1. Iniciar a execução das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução de segurança de acordo com os prazos definidos no cronograma (Anexo III), contados a partir da emissão de Ordem de Serviço - OS pelo CONTRATANTE.

7.2.2. No 3º (terceiro) dia após a emissão da Ordem de Serviço, deverá ser realizada reunião presencial na SEDE do CONTRATANTE, com o objetivo de apresentar sua metodologia de trabalho, planejamento e coordenação das atividades de entrega da solução integrada de segurança.

7.2.3. A CONTRATADA deverá apresentar um Plano de Implantação, em até 15 (quinze) dias da emissão da Ordem de Serviço pelo CONTRATANTE, contendo a documentação detalhada das atividades de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução integrada de segurança.

7.2.4. Caso a solução a ser fornecida, seja diferente da atualmente instalada, a CONTRATADA deverá providenciar a instalação dos produtos, inventariar todas configurações atualmente aplicadas no ambiente do CONTRATANTE bem como migrar todas as políticas, regras de exceção e aplicar todas as demais configurações de proteção utilizadas pelo órgão.

7.2.5. Caso a solução seja a mesma já existente, a mesma deve ser atualizada para última versão disponível e toda a configuração revisada e correções ou melhorias deverão ser implementadas.

7.2.6. O processo de instalação, atualização ou migração da solução deverá ser acompanhado pela equipe técnica indicada pelo CONTRATANTE.

7.2.7. Para garantir que a instalação, atualização ou migração não afetará o ambiente do CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos qualificados pelo fabricante nos produtos envolvidos, comprovado no ato de entrega do PLANO DE IMPLANTAÇÃO.

7.2.8. O Plano de Implantação deverá dispor também sobre o cronograma de execução, previsão de recursos humanos e materiais, pessoas envolvidas e atividades a serem desenvolvidas pela CONTRATADA e indicar os principais riscos e forma de mitigação, contendo também os seguintes itens:

a) Detalhar os procedimentos para entrega, retirada das embalagens e conferência dos equipamentos, softwares e acessórios entregues.

b) Detalhar informações sobre as etapas de instalação física dos equipamentos, incluindo: distribuição dos equipamentos pelos racks, movimentação de equipamentos existentes, conexões elétricas e lógicas necessárias, definição de nomes dos equipamentos e endereçamento de gerência IP.

c) Documentar a atual topologia física e lógica da rede LAN do CJF e propor, se necessário, nova topologia física e lógica com base nas melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução, interligando-os aos ativos de rede existentes no CJF.

d) Planejar a engenharia de tráfego da rede CJF, com base nas melhores práticas de segurança e considerando os recursos disponíveis nos elementos da solução.

e) Documentar regras e configurações atuais aplicadas aos ativos de segurança existentes no CONTRATANTE e planejar a aplicação destas regras e configurações nos equipamentos e softwares da solução integrada de segurança, eliminado as regras inativas ou desnecessárias, mediante aprovação do CONTRATANTE.

f) Indicar de forma detalhada as condições de rollback de cada mudança no ambiente do CJF.

g) Elaborar atividades de teste de operação da solução e planos de testes para os diversos componentes da solução que comprovem o funcionamento das regras e configurações aplicadas, bem como dos recursos de tolerância a falhas dos equipamentos e softwares da solução integrada de segurança.

h) Planejamento para atualização da solução atual ou migração de todas políticas, regras de exceção e todas as demais configurações de proteção atuais para a nova solução.

7.2.9. Entregar todos os equipamentos, licenças de softwares e acessórios no prazo máximo de até **45 (quarenta e cinco) dias**, a contar da data de emissão da Ordem de Serviço pelo CONTRATANTE.

7.2.10. Entregar os equipamentos novos e de 1º uso juntamente com todos os itens acessórios de hardware e de software necessários à perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, suportes, drivers de controle e programas de configuração, conforme especificações constantes do ANEXO I deste Termo de Referência.

7.2.11. Entregar os equipamentos devidamente protegidos e embalados, originais e lacrados, os quais devem evitar danos de transporte e manuseio.

7.2.12. Desembalar os equipamentos após a entrega nas dependências do CONTRATANTE.

7.2.13. Entregar os equipamentos e softwares, a suas expensas, bem como instalar e realizar todos os testes necessários à verificação do perfeito funcionamento dos produtos fornecidos.

7.2.14. Entregar todos os documentos comprobatórios de garantia indicados no item 7.4.8.

7.2.15. Entregar toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização.

7.2.16. Instalar os equipamentos e softwares nas datas e horários definidos no Plano de Implantação, sob supervisão da equipe técnica do CONTRATANTE.

7.2.17. Aceitar que as atividades de instalação, configuração dos equipamentos e softwares e operação assistida ON-SITE da solução integrada de segurança deverão ser executadas por equipe multidisciplinar, composta por técnicos plenamente qualificados na solução que será fornecida. A equipe da CONTRATADA deverá possuir certificação emitida pelos fabricantes dos equipamentos e softwares da solução ofertada e deverá ser capaz de configurar os componentes da atual infraestrutura do CJF, conforme equipamentos, modelos e versões informados no ANEXO II - Ambiente Tecnológico do CJF.

7.2.18. Aceitar que as atividades de instalação e configuração dos equipamentos e softwares da solução integrada de segurança deverão ocorrer localmente nas dependências do CJF, devendo ser realizada em horários que não coincidam com o expediente do CONTRATANTE. O CJF poderá autorizar a realização de atividades durante o horário de expediente se, ao seu exclusivo critério, entender que não oferece risco ao funcionamento de sua rede de computadores e serviços em produção.

7.2.19. Aceitar que o processo de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança da solução deverá ser acompanhado pela equipe técnica indicada pelo CONTRATANTE.

7.2.20. Aceitar que caso a implantação de qualquer elemento da solução integrada de segurança cause interferência na correta operação da rede de dados do CJF, a CONTRATADA deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação.

7.2.21. A execução dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança deverão contemplar, no mínimo, os seguintes itens:

a) Instalação física e ativação dos equipamentos da solução.

b) Realizar, se necessário, a movimentação de equipamentos e racks previamente existentes no Datacenter, caso este cenário implique na melhor configuração e organização do ambiente do CONTRATANTE.

c) Realizar a integração dos equipamentos da solução a rede LAN existente no CJF, sem interrupção no funcionamento normal dos serviços de TI. Caso exista a necessidade de interrupção de qualquer equipamento ou serviço em produção para a integração dos equipamentos, o prazo para realização e a duração da janela de manutenção deverão ser acordados com o CJF.

d) Instalar e configurar todas as funcionalidades exigidas na especificação técnica da solução, bem como quaisquer outras disponíveis adicionalmente nos diversos componentes da solução mediante solicitação da equipe do CJF.

e) Aplicar nos elementos da solução integrada de segurança todas as configurações existentes nos ativos de segurança do CONTRATANTE.

f) Realizar testes de operação da solução que comprovem o funcionamento dos recursos de tolerância a falhas das soluções de segurança.

g) Atualizar o plano de implantação com todas as informações que represente a topologia física e lógica, a configuração final e as regras aplicadas aos equipamentos e softwares da solução integrada de segurança.

7.2.22. Receber cópia do Termo de Recebimento Provisório (TRP) após entrega dos equipamentos, softwares, acessórios, Plano de Implantação e demais documentações da solução, conforme descrito no cronograma do ANEXO III. A finalização da entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

7.2.23. Concluir no prazo de 15 (quinze) dias corridos, contados a partir da emissão do Termo de Recebimento Provisório, os serviços de instalação e configuração dos equipamentos e softwares da solução integrada de segurança, realizando todas as atividades programadas para esta etapa.

7.2.24. Receber cópia do Termo de Recebimento Definitivo (TRD), após a formalização por escrito da CONTRATADA referente à conclusão das atividades de entrega, instalação e configuração dos equipamentos e softwares da solução integrada de segurança. O recebimento definitivo realizar-se-á no prazo máximo de 10 (dez) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.

7.2.25. Realizar, por 15 (quinze) dias corridos após a emissão do Termo de Recebimento Definitivo (TRD), operação assistida ON-SITE da solução de segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução.

a) O período de operação assistida ON-SITE da solução de segurança deverá ser executado presencialmente nas instalações do CJF, 3 (três) horas por dia, no período entre 14h e 21h.

b) O período de operação assistida ON-SITE faz parte dos serviços de instalação e configuração, não representando ônus adicional para o CONTRATANTE.

7.3. **Quanto ao serviço de transferência de conhecimento**

7.3.1. LOTE 01 - A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE por meio de treinamento nas tecnologias da solução com carga horária total de no mínimo 80 (oitenta) horas.

a) A transferência de conhecimento deverá abordar, no mínimo, as seguintes funcionalidades da solução:

i. Gerenciamento Unificado de Ameaças.

ii. Filtro de Conteúdo.

iii. Balanceamento de Carga.

iv. Prevenção de Intrusão.

v. Ataques avançados.

vi. Segurança para ambiente virtual.

vii. Gerenciamento e elaboração de relatórios da solução.

7.3.2. LOTE 02 - A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE por meio de treinamento nas tecnologias da solução com carga horária total de no mínimo 40 (quarenta) horas.

a) A transferência de conhecimento deverá abordar, no mínimo, as seguintes funcionalidades da solução:

i. Firewall de Aplicação.

ii. Gerenciamento e elaboração de relatórios da solução.

7.3.3. LOTE 03 - A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE por meio de treinamento nas tecnologias da solução com carga horária total de no mínimo 20 (vinte) horas.

a) A transferência de conhecimento deverá abordar, no mínimo, as seguintes funcionalidades da solução:

i. Gestão de Vulnerabilidades.

ii. Gerenciamento e elaboração de relatórios da solução.

7.3.4. O serviço de transferência de conhecimento será solicitado sob demanda, mediante de emissão de ordem de serviço.

7.3.5. A transferência de conhecimento deverá iniciar no prazo máximo de 15 (quinze) dias corridos após a emissão da ordem de serviço.

7.3.6. A transferência de conhecimento deverá ser realizada em Brasília/DF, cabendo a CONTRATADA providenciar as instalações para este fim. A transferência de conhecimento poderá ser realizada na sede do CONTRATANTE deste seja do interesse deste.

7.3.7. O programa para a transferência de conhecimento deverá ser de natureza teórica e prática, devendo abranger os equipamentos e softwares fornecidos em seus aspectos relacionados à solução implantada no ambiente computacional do Conselho, contendo, no mínimo:

a) Orientação sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE.

b) Descrição do hardware e software de cada equipamento.

c) Configuração e administração dos equipamentos.

d) Descrição geral da plataforma de gerência.

e) Diagnóstico de problemas.

f) Configuração de alarmes, eventos e rotinas para os serviços de monitoramento.

g) Gerência de desempenho e segurança.

h) Manipulação de objetos MIB, SNMP e RMON para monitoração.

i) Resolução de problemas "troubleshooting".

j) Relatórios de acesso.

7.3.8. O programa para a transferência de conhecimento deverá ser previamente aprovado pelo CONTRATANTE, e eventuais mudanças de conteúdo solicitadas deverão constar no material didático.

7.3.9. Deverá ser disponibilizado material didático impresso e em formato eletrônico, sem custo adicional para o CONTRATANTE, devendo ainda estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).

7.3.10. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.

7.3.11. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a emissão da Ordem de Serviço na primeira reunião de planejamento.

7.3.12. Caso a transferência de conhecimento não seja satisfatória com relação à profundidade do conteúdo apresentado ou domínio dos temas por parte do instrutor, a CONTRATADA deverá complementar, sem ônus adicional, o repasse dos pontos considerados pelo CONTRATANTE como insatisfatórios.

7.3.13. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelos fabricantes dos equipamentos e softwares da solução ofertada.

7.4. **Quanto ao serviço de garantia da solução**

7.4.1. O prazo de garantia dos equipamentos e direito a atualização dos softwares que compõe a solução é de 60 (sessenta) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução.

7.4.2. Todos os equipamentos e softwares fornecidos deverão suportar a última versão de firmware disponibilizada pelos fabricantes durante toda a vigência do contrato.

7.4.3. Os custos relativos ao serviço de garantia dos equipamentos e softwares que compõe a solução já devem estar incluídos no preço dos próprios itens.

7.4.4. O serviço de garantia técnica da solução consiste em reparar eventuais falhas de funcionamento dos equipamentos, dos softwares e na integração entre os componentes da solução, mediante a substituição de equipamentos e versões dos softwares ou revisão de configurações, de acordo com as recomendações dos fabricantes, informações presentes nos páginas e manuais de suporte e normas técnicas específicas.

7.4.5. O direito a atualização dos softwares obriga a CONTRATADA a disponibilizar a atualização de bases externas de categorização de sites, mensagens, vírus, malware, assinatura de ataques e vulnerabilidades, bem como dos demais softwares fornecidos e que compõe a solução, tão logo ocorra o lançamento de novos softwares em substituição aos fornecidos, ou mesmo não sendo uma substituição, se ficar caracterizada uma descontinuidade dos softwares fornecidos.

7.4.6. A reparação de falhas de funcionamento dos componentes da solução deverá ocorrer de acordo com os seguintes princípios:

a) Quanto aos equipamentos da solução:

i. Dispor de estoque de peças e equipamentos de reposição, visando à prestação dos serviços de reparação do funcionamento dos equipamentos durante todo o período de garantia.

ii. Substituir, no prazo de 8 (oito) horas, partes e componentes dos equipamentos que apresentem defeito por outras de características idênticas ou superiores, originais e novas.

iii. Nos casos em que não seja possível o reparo dentro do prazo estipulado acima, substituir no prazo máximo de 72 (setenta e duas) horas, em caráter temporário ou definitivo, o equipamento defeituoso por outro de mesma marca e modelo e com as mesmas características técnicas, novo e de primeiro uso.

iv. Substituir, no prazo de 120 (cento e vinte) horas, qualquer equipamento, componente ou periférico por outro original e novo, na ocorrência dos seguintes casos:

- Se for constatada qualquer divergência com as especificações técnicas descritas na proposta técnica apresentada.
- Se no período de 15 (quinze) dias corridos, contados após a abertura de chamado de Suporte Técnico, ocorrerem defeitos recorrentes que não permitam seu correto funcionamento, mesmo tendo havido substituição de partes e componentes.

v. Em todas as hipóteses de substituição previstas anteriormente, caso exista a impossibilidade técnica de substituição por modelo igual, novo e original, será permitida a substituição por outro com características técnicas idênticas ou superiores, plenamente compatível, também original e novo.

vi. Devolver, em perfeito estado de funcionamento, no prazo máximo de 15 (quinze) dias corridos, a contar da data de retirada dos equipamentos, os equipamentos que necessitem ser temporariamente retirados para reparo, ficando a remoção, o transporte e a substituição sob inteira responsabilidade da CONTRATADA.

vii. Responsabilizar-se pelas ações executadas ou recomendadas por analistas e consultores do quadro da empresa, assim como pelos efeitos delas advindos na execução das atividades previstas neste Termo de Referência ou no uso dos acessos, privilégios ou informações obtidas em função das atividades por estes executadas.

viii. Comunicar, por escrito, ao CONTRATANTE, sempre que constatar condições inadequadas de funcionamento ou má utilização a que estejam submetidos os equipamentos objeto deste Termo de Referência, fazendo constar a causa de inadequação e a ação devida para a correção.

b) Quanto aos softwares da solução:

i. A CONTRATADA deverá promover o isolamento, identificação e caracterização de falhas nos softwares da solução consideradas "*bug de software*".

ii. Será considerado pelo CONTRATANTE como "*bug de software*" o comportamento ou característica dos softwares que se mostrem diferentes daqueles previstos na documentação do produto e sejam considerados como prejudiciais ao seu correto uso.

iii. Serão de exclusiva responsabilidade da CONTRATADA o encaminhamento da falha de software ao laboratório do fabricante, o acompanhamento da solução e a aplicação dos respectivo fix, patch ou pacote de correção em dia e horário a ser definido pelo CONTRATANTE.

c) Quanto a integração dos componentes da solução:

i. A CONTRATADA deverá manter, durante a vigência da garantia, a correta integração entre os elementos de hardware e software que compõe a solução, nas mesmas condições de desempenho e confiabilidade que apresentavam no momento de emissão do Termo de Recebimento Definitivo.

ii. Quando forem identificadas falhas de funcionamento na solução que não sejam atribuídas diretamente aos elementos de hardware ou de software, caberá à CONTRADADA a análise e o encaminhamento da solução, buscando restaurar o correto funcionamento do conjunto de elementos da solução.

iii. Serão consideradas como falhas de funcionamento da integração dos componentes a redução significativa do desempenho ou a perda de funcionalidades técnicas disponibilizadas pelo conjunto da solução.

7.4.7. A atualização dos softwares fornecidos que compõe a solução deverá ocorrer de acordo com os seguintes princípios:

a) O CONTRATANTE deverá ter direito irrestrito, durante a vigência da garantia, de atualizar as bases externas de categorização de sites, mensagens, vírus, malware, assinatura de ataques e vulnerabilidades.

b) O CONTRATANTE deverá ter direito irrestrito, durante a vigência da garantia, de atualizar as versões de todos os softwares que compõe a solução, mesmo que os fabricantes alterem suas políticas de licenciamento dos softwares.

c) O direito a atualização de versões dos softwares que compõe a solução não poderá gerar qualquer custo adicional para o CONTRATANTE.

d) Deverão ser criadas contas de acesso, em nome do CONTRATANTE, no sítio internet do fabricante dos softwares que compõe a solução.

e) O perfil das contas criadas em nome do CONTRATANTE deverá permitir de forma irrestrita o download de drivers, firmwares, patches, atualizações, novas versões, informações de suporte, acesso a base de conhecimento e manuais técnicos.

f) Sempre que solicitado mediante chamado de Suporte Técnico, a CONTRATADA deverá orientar o CONTRATANTE quanto aos procedimentos técnicos para a instalação ou atualização de versões dos softwares que compõe a solução.

7.4.8. Juntamente com a documentação de entrega, instalação e configuração da solução, como requisito para a emissão do Termo de Recebimento Definitivo, a CONTRATADA deverá entregar a seguinte documentação:

a) Certificado de garantia de que todos os equipamentos que compõe a solução estão cobertos por garantia e suporte técnico on-site, diretamente do fabricante, com prazo de solução de até 8 (oito) horas, pelo período de 60 (sessenta) meses totais exigidos no item 7.4.1.

i. Caso não seja comercializado item de garantia com o prazo nos moldes exigidos no item anterior, deverá ser entregue pela CONTRATADA declaração oficial, emitida pelo fabricante dos equipamentos, atestando a contratação do serviço de garantia e suporte técnico on-site com o nível de serviço e duração solicitados.

b) Cessões de direito de uso perpétuo dos softwares fornecidos. Os termos de licenciamento de todos os softwares fornecidos, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e os mesmos serão direito pertencentes ao CONTRATANTE.

c) Conjunto de direitos de atualização de versão, pelo período de 60 (sessenta) meses de garantia, de todos os softwares fornecidos. Abrangerá todos os softwares e licenças a serem fornecidos na solução. Os termos de

licenciamento referentes aos direitos de atualização de versão, emitidos pelo fabricante, deverão ser entregues pela CONTRATADA e comporão patrimônio do CONTRATANTE.

7.5. **Quanto ao serviço de suporte técnico**

7.5.1. O serviço de suporte técnico on-site para os equipamentos e softwares que compõe a solução deverá ser executado pela CONTRATADA ou diretamente pelo fabricante, durante o prazo de 60 (sessenta) meses, contados a partir da data de aceitação pelo CONTRATANTE, ou seja, emissão do Termo de Recebimento Definitivo dos serviços de entrega, instalação e configuração dos equipamentos e softwares da solução.

7.5.2. O serviço de suporte técnico da solução consiste em:

a) Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, no local de instalação da solução, visando à solução de problemas que afetem de forma isolada ou conjunta, qualquer elemento da solução (equipamentos e softwares), permitindo o retorno à condição normal de operação.

b) Atuar, mediante abertura pelo CONTRATANTE de chamado técnico de suporte, por meio de contato telefônico ou outros recursos de comunicação, visando o esclarecimento de dúvidas em relação a qualquer elemento da solução.

c) Realizar visitas técnicas preventivas no local de instalação da solução (on-site), com frequência mensal, e com duração de pelo menos 8 (oito) horas a cada visita, visando assegurar o melhor desempenho da solução.

d) Substituir peças e componentes, cujos problemas sejam decorrentes do desgaste pelo uso normal dos equipamentos, por outras de configuração idêntica ou superior, originais e novas.

7.5.3. Quando da abertura de chamado técnico de suporte pelo CJF, os chamados deverão ser categorizados em 4 (quatro) níveis, da seguinte forma:

Criticidade	Descrição	Prazo máximo para início de atendimento (contados a partir da abertura do chamado)	Prazo máximo para restauração de serviço (contados a partir da abertura do chamado)
Severidade 1 (Alta)	Atuação ON-SITE visando sanar problemas que tornem a solução integrada de segurança inoperante, causando alto impacto nas operações de TI do CJF.	Em até 2 (duas) horas deve ter um técnico da CONTRATADA ON-SITE	Em até 6 (seis) horas
Severidade 2 (Média/Alta)	Atuação ON-SITE visando sanar problemas que prejudicam a operação normal da solução, mas não interrompem o acesso aos sistemas de TI, causando impacto no ambiente de produção ou restrição de funcionalidade.	Em até 4 (quatro) horas deve ter um técnico da COTRATADA ON-SITE.	Em até 12 (doze) horas
Severidade 3 (Média/Baixa)	Atuação REMOTA visando sanar problemas ou dúvidas que criem restrições a operação normal da solução integrada de segurança não gerando impacto ao negócio.	Em até 4 (quatro) horas um técnico da CONTRATADA entra em contato.	Em até 24 (vinte e quatro) horas
Severidade 4 (Baixa)	Atuação REMOTA visando sanar problemas que não afetem a operação normal da solução integrada de segurança, ou dúvidas de operação e configuração.	Em até 12 (doze) horas um técnico da CONTRATADA entra em contato.	Em até 72 (setenta e duas) horas

7.5.4. O CONTRATANTE realizará a abertura de chamados técnicos de suporte por meio de ligação telefônica ou via Internet, em período integral, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

7.5.5. A CONTRATADA deverá informar o procedimento para abertura de chamado técnico de suporte no documento plano de implantação.

7.5.6. Se a Central de Suporte estiver localizada fora de Brasília, a CONTRATADA deverá informar o DDG (discagem direta gratuita 0800). O acesso à área restrita de suporte em endereço eletrônico (web site) deverá estar disponível, também, 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana.

7.5.7. Quando da abertura de chamado técnico de suporte pelo CONTRATANTE, a CONTRATADA deverá informar o número do chamado, para fins de controle.

7.5.8. A CONTRATADA deverá enviar mensalmente, ou disponibilizar acesso por meio de portal internet, relação consolidada dos chamados abertos no mês, mencionando: data e hora de abertura do chamado técnico, número do chamado técnico, problemas verificados, técnico responsável pelo atendimento.

7.5.9. A CONTRATADA deverá disponibilizar acesso total ao conteúdo presente em área restrita de suporte no endereço eletrônico (web site) para todos os produtos que compõem a solução, contemplando toda a documentação técnica (guias de instalação/configuração atualizados, FAQ's, com pesquisa efetuada através de ferramentas de busca) e atualizações.

7.5.10. A CONTRATADA deverá realizar a cada ocorrência, como escopo das atividades de visitas técnicas preventivas, as tarefas de coleta e análise de logs dos produtos, realizar o levantamento de configurações aplicadas nos equipamentos e softwares que compõe a solução integrada de segurança, buscando compará-las às melhores práticas e recomendações dos fabricantes, avaliar aspectos de segurança e desempenho da solução, finalizando com a elaboração de relatório técnico com as informações coletadas e as recomendações a serem aplicadas à solução.

7.5.11. As visitas técnicas preventivas deverão ser realizadas por técnico(s) plenamente qualificado(s) nas áreas de gerenciamento de ameaças, análise de vulnerabilidades e firewall de aplicação, devendo possuir certificação emitida pelos fabricantes dos equipamentos e softwares da solução ofertada. As visitas técnicas serão prestadas com acompanhamento da equipe técnica do CJF.

7.5.12. A contagem de prazo para a realização das visitas técnicas preventivas será iniciada após emissão do Termo de Recebimento Definitivo da solução, devendo ocorrer automaticamente em dia e hora previamente agendada com o CJF e serão consideradas concluídas após o entrega do relatório técnico de atendimento e aceite pelo CJF. A cada visita deverá ser gerado relatório técnico com sugestões e ajustes para a melhoria de desempenho, aplicação de funcionalidade e revisão dos aspectos de segurança.

7.5.13. A CONTRATADA deverá prestar as informações e os esclarecimentos que venham a ser solicitados pelos técnicos do CJF, em relação à instalação, configuração e problemas detectados, atendendo de imediato as solicitações.

8. OBRIGAÇÕES DO CONTRATANTE

8.1. Acompanhar e fiscalizar a execução do objeto contratual.

8.2. Determinar responsável para o acompanhamento e fiscalização da execução do objeto contratual.

8.3. Informar a CONTRATADA de atos que possam interferir direta ou indiretamente nos serviços prestados.

8.4. Comunicar formalmente qualquer anormalidade ocorrida na execução dos serviços pela CONTRATADA.

8.5. Avaliar todos os serviços prestados pela CONTRATADA.

8.6. Responsabilizar-se pelos pagamentos dos serviços prestados pela CONTRATADA mediante a apresentação de Nota Fiscal.

8.7. Indicar os seus representantes para fins de contato e demais providências inerentes à execução do contrato.

8.8. Para os serviços inclusos no período de garantia do objeto, o CONTRATANTE permitirá o acesso dos técnicos habilitados e identificados da CONTRATADA às instalações onde se encontrarem os equipamentos. Esses técnicos ficarão sujeitos a todas as normas internas de segurança do CONTRATANTE, inclusive aquelas referentes à identificação, trânsito e permanência em suas dependências.

9. UNIDADE GESTORA/ FISCALIZADORA DO CONTRATO

9.1. O Chefe da Seção de Segurança de Rede (SESERE) será o gestor do contrato e acompanhará sua execução, devendo proceder a orientação, fiscalização e interdição da sua execução, se necessário, a fim de garantir o exato cumprimento das condições estabelecidas em contrato.

9.2. O representante da Área Administrativa (Fiscal Administrativo do Contrato), indicado pela autoridade competente dessa área, fiscalizará o contrato quanto aos aspectos administrativos, tais como a verificação de regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento.

10. FORMA DE PAGAMENTO

10.1. A CONTRATADA deverá emitir Notas Fiscais/Faturas relativas aos valores dos equipamentos e softwares da solução e garantia por 60 (sessenta) meses, serviços de instalação e configuração e serviço de transferência de conhecimento após receber cópia do Termo de Recebimento Definitivo previsto no Cronograma (ANEXO III).

10.2. O pagamento do serviço de Suporte Técnico será efetuado mensalmente, sendo iniciado somente após o Recebimento Definitivo da Solução, mediante envio da Nota Fiscal/Fatura pela CONTRATADA.

10.3. O pagamento será realizado no prazo de até 10 (dez) dias úteis contados a partir do recebimento da nota fiscal.

10.4. O servidor indicado para a fiscalização da presente aquisição terá o prazo de 5 (cinco) dias para "ATESTAR" a Nota Fiscal ora mencionada, após a data de apresentação do referido documento a este Órgão.

10.5. A nota Fiscal deverá ser apresentada na Seção de Protocolo e Expedição - SEPEX deste Conselho.

11. VIGÊNCIA

11.1. A vigência do Contrato será de:

11.1.1. 4 (quatro) meses, contados da assinatura do contrato, para a execução, mediante a emissão da Ordem de Serviços, da entrega, instalação, configuração, transferência de conhecimento e recebimento definitivo.

11.1.2. 60 (sessenta) meses, contados da data de emissão do Termo de Recebimento Definitivo, referente aos serviços de garantia e suporte técnico da solução integrada de segurança, relativo aos serviços de natureza contínua desta contratação.

12. LOCAIS DE ENTREGA E INSTALAÇÃO DOS PRODUTOS

12.1. A entrega dos equipamentos, softwares e acessórios da solução e a realização dos serviços previstos neste contrato deverão ser realizados na sede do CONTRATANTE, situada no Setor de Clubes Esportivos Sul - SCES - Trecho III - Pólo 8 - Lote 9 - CEP 70200-003 - Brasília/DF.

13. MODELO DE REMUNERAÇÃO (Glosas)

13.1. O não cumprimento dos níveis de qualidade do Serviço de Suporte Técnico por ocorrência, independentemente das Sanções Administrativas previstas no Contrato, implicará em redutor na fatura mensal do serviço de suporte técnico (glosa), nos seguintes casos:

13.1.1. Glosa de 6% (seis por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com **severidade alta**, limitada até 06 (seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.2. Glosa de 3% (três por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com severidade **média/alta**, limitada até 12 (doze) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.3. Glosa de 2% (dois por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com severidade **média/baixa**, limitada até 18 (dezoito) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.4. Glosa de 1% (um por cento), calculada sobre o valor do serviço de suporte técnico da solução, para cada hora de atraso, pela não resolução dos chamados com severidade **baixa**, limitada até 36 (trinta e seis) horas de atraso, quando se aplicará o percentual de 30% (trinta por cento).

13.1.5. Nos casos em que os atrasos forem superiores aos limites previstos nos subitens anteriores, além da aplicação das glosas previstas, poderá ser aberto processo específico pelo CONTRANTE para apuração de uma possível aplicação de penalidade.

13.2. A aplicação da glosa servirá ainda como indicador de desempenho da CONTRATADA na execução dos serviços.

13.3. O faturamento do serviço de suporte técnico deverá ser mensal, mediante apresentação de nota de cobrança consolidada para todos os equipamentos e softwares da solução, já descontadas as glosas eventualmente aplicadas em função do não atendimento dos níveis de qualidade definidos no contrato, determinando o valor total do serviço para o mês.

13.4. No caso de aplicação de glosa referente à demora na conclusão de chamados do mesmo nível de severidade, para qualquer componente da solução, durante 3 (três) meses consecutivos ou 5 (cinco) meses intervalados, durante os últimos 12 (doze) meses, será aberto processo específico para apuração de uma possível aplicação de penalidade.

13.5. No caso de discordância das glosas aplicadas, a CONTRATADA deverá apresentar o recurso que será analisado pela Área Administrativa

13.6. Se a decisão da Administração for favorável ao recurso da CONTRATADA, a mesma emitirá a nota de cobrança adicional para que seja efetuado o pagamento referente ao valor glosado.

13.7. A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo Gestor do Contrato e encaminhada para a área financeira efetuar o pagamento, acompanhada da documentação comprobatória das glosas.

14. DAS PENALIDADES

14.1. Pela inexecução total ou parcial das obrigações assumidas a Administração poderá, resguardados os procedimentos legais pertinentes, aplicar as seguintes sanções:

14.1.1. Advertência.

14.1.2. Multa no percentual correspondente a 0,05% (cinco centésimos por cento), calculada sobre o valor total da contratação, **por dia de atraso na entrega do plano de implantação**, além do prazo máximo definido no CRONOGRAMA (ANEXO III), até o limite de 30 (trinta) dias corridos.

14.1.3. Multa no percentual correspondente a 0,1% (um décimo por cento), calculada sobre o valor total da contratação, **por dia de atraso na entrega de todos os equipamentos, softwares e acessórios da solução**, além do prazo máximo definido no CRONOGRAMA (ANEXO III), até o limite de 30 (trinta) dias corridos, caracterizando inexecução total do contrato.

14.1.4. Multa no percentual correspondente a 0,1% (um décimo por cento), calculada sobre o valor total da contratação, **por dia de atraso na conclusão da etapa de instalação e configuração da solução**, além dos prazos máximos definidos no CRONOGRAMA (ANEXO III) até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

14.1.5. Multa no percentual correspondente a 0,5 (meio por cento), calculada sobre o valor total do serviço de transferência de conhecimento, **por dia de atraso na conclusão do serviço de transferência de conhecimento**, além do prazo máximo definido no CRONOGRAMA (ANEXO III), até o limite de 30 (trinta) dias corridos, caracterizando inexecução parcial do contrato.

14.1.6. Multa no percentual correspondente a 20% (vinte por cento), calculada sobre o valor do suporte técnico mensal, **no caso de aplicação de glosa referente ao mesmo indicador de Nível Mínimo de Serviço, durante 3 (três) meses consecutivos, ou 5 (cinco) meses intervalados durante os últimos 12 meses**, caracterizando inexecução parcial do contrato.

14.1.7. Multa no percentual correspondente a 0,20% por dia de atraso, até o limite de 30 (trinta) dias corridos, calculada sobre o valor da garantia contratual disposta no item 19.1 deste Termo, **no caso de atraso injustificado na sua entrega.**

14.1.8. A inexecução parcial deste instrumento, por parte da CONTRATADA, poderá ensejar a rescisão contratual ou a aplicação da multa, no percentual de 10% (dez por cento) sobre o valor da parte não entregue ou não executada.

14.1.9. Multa no valor de 10% (dez por cento), sobre o valor total da contratação, **no caso de inexecução total do contrato**.

14.1.10. O disposto nos itens anteriores não prejudicará a aplicação de outras penalidades a que esteja sujeita a CONTRATADA, nos termos dos artigos 87 e 88 da Lei n. 8.666/1993.

14.2. O valor da multa aplicada, após regular procedimento administrativo, será descontado dos pagamentos eventualmente devidos pelo CONTRATANTE, descontado da garantia contratual ou cobrado judicialmente.

14.3. A reincidência da aplicação de multa ou advertência dará direito ao CJF à rescisão contratual unilateral.

14.4. As sanções serão obrigatoriamente registradas no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

14.5. SUSPENSÃO TEMPORÁRIA- suspender temporariamente de participação em licitação e impedimento de contratar com a União, nos termos do art. 7º da Lei n. 10.520/2002 c/c o art. 28 do Decreto n. 5.450/2005.

14.6. SUSPENSÃO TEMPORÁRIA - pela inexecução total ou parcial do objeto será suspensa temporariamente de participar de licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos, nos termos inciso 3 do artigo 87 na lei de Licitação 8666/93, bem como conforme Acórdão 2242/2013.

15. CONFIDENCIALIDADE

15.1. A CONTRATADA compromete-se a manter em caráter confidencial, mesmo após a eventual rescisão do contrato, todas as informações relativas à:

15.1.1. Política de segurança adotada pelo CJF e configurações de hardware e software decorrentes.

15.1.2. Processo de instalação, configuração e customizações de produtos, ferramentas e equipamentos em atendimento aos itens de segurança constantes do(s) objeto(s) instalado(s)

15.2. A CONTRATADA deverá concordar e assinar Termo de Confidencialidade e Sigilo da Contratada (ANEXO VII), entregando o Termo assinado pelo representante legal da empresa, com firma reconhecida.

16. VISTORIA

16.1. A LICITANTE, caso julgue conveniente para o correto dimensionamento e cumprimento das obrigações, poderá realizar uma vistoria nas instalações do CONTRATANTE para tomar conhecimento dos serviços a serem realizados. Não serão admitidas, em hipótese alguma, alegações posteriores de desconhecimento dos serviços e de dificuldades técnicas não previstas:

16.1.1. A vistoria técnica deverá ocorrer por horário marcado, e será agendada por meio do telefone (61) 3022-7400/7403.

16.1.2. O agendamento de vistoria poderá ocorrer até 60 (sessenta) horas antes da data e horário de abertura do processo licitatório.

16.1.3. A vistoria técnica deverá ser realizada em até, no máximo, 24 (vinte e quatro) horas da abertura do processo licitatório.

16.1.4. Detalhes da topologia lógica da rede de dados do CONTRATANTE serão apresentados durante a vistoria somente mediante assinatura de Termo de Confidencialidade e Sigilo do Licitante (ANEXO VI), a ser preenchido e assinado pelo representante legal da empresa.

17. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

17.1. A LICITANTE vencedora deverá fornecer declaração comprometendo-se a prestar garantia de, no mínimo, 60 (sessenta) meses a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).

17.2. A LICITANTE deverá ofertar Suporte Técnico pelo período de 60 (sessenta) meses, a contar da data de recebimento do Termo de Recebimento Definitivo (TRD).

17.3. A proposta deverá indicar, em qual página e item da documentação apresentada, está a comprovação do atendimento dos requisitos técnicos descritos no ANEXO I deste Termo de Referência. Não será aceita proposta sem a indicação na documentação técnica apresentada.

17.4. A proposta deverá incluir, em versão eletrônica, todos os catálogos ou prospectos do fabricante ou da internet, preferencialmente em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês), correspondente aos produtos ofertados, com descrição detalhada de cada item.

17.5. Todos os equipamentos e softwares especificados deverão ser adquiridos em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo com o término do contrato.

17.6. A LICITANTE vencedora do LOTE 01 deverá apresentar atestado(s) de capacidade técnica, que comprove que a empresa LICITANTE tenha fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução englobando o fornecimento de solução de gerenciamento de ameaças (UTM), solução contra ameaças avançadas (APT) e solução de segurança multifunção para ambiente virtualizado.

17.7. A LICITANTE vencedora do LOTE 02 deverá apresentar atestado(s) de capacidade técnica, que comprove que a empresa LICITANTE tenha fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução de firewall de aplicação web.

17.8. A LICITANTE vencedora do LOTE 03 deverá apresentar atestado(s) de capacidade técnica, que comprove que a empresa LICITANTE tenha fornecido e implementado a contento, para órgãos ou entidades públicas ou privadas, solução de gerenciamento de vulnerabilidades de TI.

17.9. Deverão constar do(s) atestado(s) de capacidade técnica em destaque, os seguintes dados: identificação do emitente, especificação completa do fornecimento/serviço executado, prazo de vigência do contrato, local e data de expedição, data de início e término do contrato.

18. PROVA DE CONCEITO

18.1. Poderá ser solicitada, a critério exclusivo do CJF, prova de conceito à empresa classificada, antes da adjudicação, com o objetivo de realizar testes de comprovação de atendimento às especificações e requisitos exigidos nas Especificações Técnicas deste Termo de Referência caso a documentação entregue pela LICITANTE seja considerada insuficiente para comprovar o atendimento a todos os itens exigidos.

18.2. Para a realização da prova de conceito a LICITANTE deverá disponibilizar conjunto de elementos que atendam as especificações detalhadas na proposta.

18.3. A realização da prova de conceito deverá ser presencial e realizada, preferencialmente, na Secretaria de Tecnologia da Informação do CJF, localizada no SCES Trecho 03 Pólo 08 Lote 09, CEP 70200-003, Brasília - DF, em dias úteis, ou, a critério exclusivo do CJF e mediante exposição de motivos, em qualquer cidade brasileira, devendo iniciar no prazo de até 05 (cinco) dias úteis, contados a partir da data de convocação do CONTRATANTE para a realização da prova de conceito.

18.4. O CONTRATANTE, a seu critério, poderá prorrogar a duração da prova de conceito por mais 02 (dois) dias úteis

18.5. A prova de conceito utilizará como base as especificações técnicas constantes neste Termo de Referência.

18.6. Será rejeitada a prova de conceito que:

18.6.1. Não comprovar o atendimento de, pelo menos, 01 (um) requisito técnico descrito no ANEXO I - Especificações Técnicas deste Termo de Referência, executada nos equipamentos e softwares entregues para a prova de conceito.

18.6.2. Apresentar divergências entre as especificações dos equipamentos e softwares entregues para a prova de conceito em relação às especificações técnicas da proposta entregue pela LICITANTE.

18.7. Não será aceita a proposta da LICITANTE que tiver a prova de conceito rejeitada ou não entregue no prazo estabelecido.

18.8. Nesse caso, a proposta subsequente será examinada e, assim, sucessivamente, na ordem de classificação, até a aprovação de uma prova de conceito.

19. GARANTIA DO CONTRATO

19.1. Para assegurar o integral cumprimento de todas as obrigações contratuais assumidas, inclusive indenização a terceiros e multas eventualmente aplicadas, a CONTRATADA se obriga a oferecer, como prestação de garantia, o valor correspondente a 5% (cinco por cento) do valor total contratado, no prazo máximo de 20 (vinte) dias, contados a partir da assinatura do contrato.

19.1.1. A CONTRATADA ficará obrigada a apresentar nova garantia sempre que necessário, seja por expirar o vencimento, alteração por aumento no valor do contrato ou outra necessidade indispensável.

19.2. Não serão aceitos instrumentos de garantia que contenham cláusulas conflitantes com dispositivos contratuais ao até mesmo restrinjam-lhe a cobertura ou a sua eficácia.

19.3. O termo da garantia será restituído à CONTRATADA depois de encerrada a vigência contratual, e após o cumprimento integral de todas as obrigações contratuais.

20. DO DESENVOLVIMENTO NACIONAL SUSTENTÁVEL

20.1. Os equipamentos fornecidos não deverão conter substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenilpolibromados (PBDEs) em concentração acima da recomendada pela diretiva da Comunidade Econômica Europeia Restriction of Certain Hazardous Substances – RoHS (Restriction of Certain Hazardous Substances).

20.2. O fabricante, importador ou distribuidor dos equipamentos deverá assegurar o recolhimento dos equipamentos que contenham materiais perigosos e declarar que dará a destinação final ambientalmente adequada.

20.3. Considerando que a indústria de material elétrico, eletrônico e comunicações se enquadra entre as atividades potencialmente poluidoras ou utilizadoras de recursos ambientais listadas no Anexo I da Instrução Normativa Ibama n. 6 de 15 de março de 2013, sujeitando a fabricante ao devido registro no Cadastro Técnico Federal. A licitante deverá informar o CNPJ da fabricante, para que, dessa forma, possa ser averiguada a regularidade do fabricante junto ao Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais – CTF.

21. DOCUMENTOS ANEXOS

21.1. Seguem anexos a este Termo de Referência os seguintes documentos:

21.1.1. Anexo I – Especificação Técnica da Solução.

21.1.2. Anexo II – Ambiente Tecnológico do CJF.

21.1.3. Anexo III – Cronograma de Implantação.

21.1.4. Anexo IV – Planilha de Preços.

21.1.5. Anexo V – Termo de Vistoria.

21.1.6. Anexo VI – Termo de Confidencialidade e Sigilo da Licitante.

21.1.7. Anexo VII – Termo de Confidencialidade e Sigilo da Contratada.

ATA DE REGISTRO DE PREÇOS N. 013/2017 - CJF

ANEXO I - ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO

A solução de segurança a ser fornecida deverá ser integrada a estrutura tecnológica em uso no CJF composta por switches core, servidores, switches topo de rack, de acordo com os modelos e versões detalhadas no documento **Ambiente Tecnológico do CJF (ANEXO II)**. Será de responsabilidade da empresa CONTRATADA o fornecimento e instalação de todos os itens acessórios de hardware e software necessários à sua perfeita instalação e funcionamento, incluindo cabos, conectores, interfaces, adaptadores, suportes, drivers de controle, programas de configuração, cordões ópticos e demais componentes necessários para a perfeita integração da solução a infraestrutura existente no CONTRATANTE.

São apresentadas, a seguir, especificações técnicas mínimas dos equipamentos a serem ofertados referentes aos LOTE 01: itens 1, 2, 3, 4 e 5; LOTE 02: item 01 e LOTE 03: item 01. Os verbos "possuir", "permitir", "suportar" e "é" implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo "ou" implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo "e" implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

Todos os componentes necessários à solução deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do CONTRATANTE.

Os componentes do LOTE 01 deverão ocupar no máximo 10U (dez unidades) de espaço no rack, considerando o somatório dos espaços utilizados por todos os componentes da solução (Itens 1, 2, 3, 4 e 5).

LOTE 01

ITEM 1 - SOLUÇÃO DE GERENCIAMENTO DE AMEAÇAS

Os equipamentos, produtos, peças ou softwares necessários à Solução de Gerenciamento de Ameaças deverão ser instalados no *datacenter* do CONTRATANTE, devendo observar os seguintes requisitos mínimos:

1.1. Ser provido com emprego de, no mínimo, 2 (dois) elementos para serem fixados em *rack* padrão 19", sendo que o conjunto dos requisitos especificados poderá ser atendido por meio de outros equipamentos.

1.2. Permitir alta disponibilidade com tolerância a falhas utilizando a configuração ativo-ativo.

1.3. Possuir fontes de alimentação hot swappable 220v, redundantes N+1.

1.4. Suportar toda a pilha IPv4/IPv6.

1.5. Permitir a aplicação de novas políticas em tempo real, sem interrupção do tráfego.

1.6. Deverão ser fornecidos manuais de operação e configuração do(s) equipamento(s) proposto(s) em português ou inglês (cabos, acessórios e programas de configuração necessários à completa operacionalização dos recursos exigidos nesta especificação.

1.7. **Na função de firewall de rede:**

1.7.1. Possuir pelo menos 4 (quatro) portas de comunicação dedicada, padrão 10GbE (10 Gigabit Ethernet).

1.7.2. Possuir pelo menos 8 (oito) portas de comunicação dedicada, padrão Gigabit Ethernet (Cobre ou 1000Base-T SFP).

1.7.3. Deverão ser fornecidos os respectivos transceivers SFP+ 10GBASE-SR, SFP, licenças de uso das portas e cordões óticos duplex MMF LC/LC, com comprimento máximo de 10m, necessários para a interligação das portas externas ao switch core do Datacenter.

1.7.4. Possuir porta independente para gerência, padrão Gigabit Ethernet (Cobre ou 1000base-T SFP ou 1000base-SX Conector LC) ou superior.

1.7.5. Possuir porta(s) independente(s) para sincronismo de cluster, padrão Gigabit Ethernet (Cobre ou 1000base-T SFP ou 1000base-SX Conector LC) ou superior.

1.7.6. Deverão ser fornecidos 20 (vinte) patch cords CAT. 6 certificados, com comprimento de pelo menos 5 (cinco) metros, necessários a interligação das portas externas ao switch core do Datacenter.

1.7.7. Possuir throughput de tráfego real de, no mínimo, 30 (trinta) Gbps (gigabits por segundo) com funcionalidade de firewall habilitada ou possuir throughput de, no mínimo, 12 (doze) Gbps (gigabits por segundo) com as funcionalidades de firewall e controle de aplicação habilitados simultaneamente.

1.7.8. Possuir throughput de tráfego real de, no mínimo, 7 (sete) Gbps (gigabits por segundo) de NGFW com, no mínimo, as funcionalidades de firewall, IPS e controle de aplicação habilitadas simultaneamente.

1.7.9. Para fins de comprovação de valores de throughput dos itens 1.7.7 e 1.7.8 serão admitidos apenas os testes realizados pela organização independente NSS Labs para o perfil de tráfego "Real World Protocol Mix (Enterprise Perimeter) ".

1.7.10. Permitir tratar 10.000.000 (dez milhões) de sessões simultâneas.

1.7.11. Permitir a admissão 180.000 (cento e oitenta mil) novas conexões por segundo.

1.7.12. Permitir no mínimo 2.000 (duas mil) regras de firewall.

1.7.13. Permitir o estabelecimento de túneis IPSec com VPN com throughput de no mínimo 10 (dez) Gbps de tráfego para criptografia usando AES 256 ou AES128.

1.7.14. Permitir a filtragem de pacotes baseada em estados (stateful inspection).

1.7.15. Permitir o registro dos fluxos de dados relativos a cada sessão iniciada, armazenando para cada uma destas os endereços de origem e destino dos pacotes, portas TCP e UDP de origem e destino, bem como números de sequência de pacotes TCP.

1.7.16. Suportar toda a pilha de protocolos do modelo TCP/IP, com as seguintes funcionalidades:

a) Fazer inspeção *stateful* de tráfego.

b) Suportar roteamento estático de tráfego.

1.7.17. Permitir o funcionamento em modo transparente tipo bridge e permitir ser configurado em alta disponibilidade neste modo.

1.7.18. Permitir a criação de regras por endereço de origem e destino, sub-rede IP, protocolo de rede, porta de destino e tipo de serviço. Também deverá permitir a identificação da interface de rede de origem, quando a tecnologia do equipamento permitir.

1.7.19. Permitir a definição de período de validade de regras, ou seja, determinar a validade de uma regra de acordo com o horário, data ou dia da semana.

1.7.20. Permitir o uso de NAT (Network Address Translation) e PAT (Protocol Address Translation).

1.7.21. Suportar tags de VLAN trunking (802.1q), sendo possível configurar pelo menos 255 (duzentas e cinqüenta e cinco) vlan-id em uma mesma interface física.

1.7.22. Permitir a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas.

1.7.23. Permitir sincronização do relógio utilizando o protocolo NTP ou SNTP para sincronizar com bases externas.

1.7.24. Permitir proteção contra-ataques de:

a) SYN Flood.

b) IP Spoofing.

c) UDP Flood.

1.7.25. Suportar os protocolos de roteamento BGP4 e OSPF v.2.

1.7.26. Possuir funcionalidade de servidor DHCP e Relay DHCP.

1.7.27. Permitir o estabelecimento de túneis (VPN site-to-site) com, no mínimo as seguintes especificações:

a) Utilizar protocolo IPSEC e IPSEC NAT traversal.

b) Efetuar troca de chaves por meio de protocolo IKE e certificados X. 509.

c) Criptografar utilizando especificação AES (256 bits).

d) Permitir a utilização de pelo menos 512 túneis simultâneos.

1.7.28. Permitir a criação dinâmica a partir da análise da sinalização H.225 e H.245 (Call Setup e Call Control, respectivamente) de regras pertinentes para tráfego de mídia (RTP/RTCP) entre as MCUs do CJF e as estações de videoconferência da Justiça Federal, consistindo tais regras em combinações de:

a) IP e porta de origem (elemento originador da chamada).

b) IP e porta de destino (elemento recipiente da chamada).

c) Interfaces de entrada e saída do tráfego de vídeo com inspeção stateful.

1.7.29. Suportar as versões 2, 3 e 4 do Framework H.323.

1.7.30. Suportar Multicast.

1.7.31. Permitir a administração por ferramenta com interface gráfica remota segura, utilizando browser.

1.7.32. Permitir a administração por interface de linha de comando (CLI – Command Line Interface) com uso de protocolo de comunicação SSHv2.

1.7.33. Permitir a replicação de configurações e a aplicação de atualização de software para os elementos dos nós do cluster.

1.7.34. Permitir a definição de diferentes níveis de administração, sendo ao menos um nível completo e outro somente de visualização de configurações e logs.

1.7.35. Caso a solução de gestão de ameaças exija servidor físico de uso genérico para a execução de qualquer de suas funcionalidades, o equipamento ofertado deverá atender aos seguintes requisitos:

a) Servidor tipo rack, para instalação em rack padrão de 19", limitado a 2U de altura.

b) Possuir pelo menos 2 (dois) processadores de 8 (oito) núcleos cada, arquitetura de 64 bits.

c) Possuir pelo menos 64GB de memória RAM DDR3.

d) Possuir pelo menos 2 (dois) discos internos com configuração mínima de 300 GB, tecnologia SAS, velocidade de 10.000 RPM.

e) Possuir pelo menos 2 (duas) portas GbE 1000Base-T.

f) Possui fonte de alimentação hot swappable 220V, redundantes N+1.

1.8. **Na função de gerência de qualidade de serviço:**

1.8.1. Permitir controle e priorização de tráfego, priorizando e garantindo banda para as aplicações através da classificação dos pacotes, criação de filas de prioridade, gerencia de congestionamento e QoS.

1.8.2. Permitir modificação de valores DSCP para o Diffserv.

1.8.3. Limitar individualmente a banda utilizada por diferentes aplicações e serviços tanto para tráfego de entrada na internet quanto de saída.

1.9. **Na função de filtro de conteúdo:**

1.9.1. Suportar no mínimo 800 usuários simultâneos.

1.9.2. Permitir a utilização de pelo menos 40 (quarenta) categorias para classificação de sites web.

1.9.3. Possuir base mínima contendo ao menos 100 (cem) milhões de sites internet web já registrados e classificados, pelo menos nos idiomas inglês, português e espanhol.

1.9.4. Permitir atualização automática de base de URLs via internet com base do fabricante durante todo o período contratual.

1.9.5. Possuir categoria exclusiva no mínimo para os seguintes tipos de sites web:

a) Compras.

b) Hacker.

c) Instituições governamentais.

d) Notícias.

e) Phishing.

f) Pornografia.

g) Proxy.

h) Racismo.

i) Redes sociais.

j) Webmail.

1.9.6. Permitir a recategorização de sites, diferente da categorização original do site.

1.9.7. Permitir monitoração do tráfego interno sem bloqueio de acesso aos usuários.

1.9.8. Permitir identificação dos usuários de maneira integrada com LDAP e Active Directory para aplicação de políticas de controle, priorização e filtragem de tráfego WEB.

1.9.9. Permitir integração com grupos ou OUs (Organizational Units) no Active Directory.

1.9.10. Permitir identificação transparente de usuários cadastrados no Active Directory, sem necessidade de entrada de usuário e senha para usuários já logados em estação de trabalho utilizando Windows 7 e 10.

1.9.11. Permitir customização de mensagens para resposta aos usuários.

1.9.12. Permitir a filtragem de conteúdo WEB de códigos (programas/scripts) maliciosos.

1.9.13. Permitir a atualização regular do produto e suas bases de dados sem interromper a execução dos serviços de filtragem.

1.9.14. Suportar Proxy do tráfego WEB a ser filtrado no mínimo nos protocolos HTTP e HTTPS.

1.9.15. Permitir a operação como Proxy explícito e transparente, de acordo com a interface.

1.9.16. Permitir filtragem de tráfego criptografado via SSL tanto na entrada como na saída, atuando como interceptor de tráfego (man-in-the-middle).

1.9.17. Suportar a verificação de certificados de URL solicitadas, permitindo bloqueio caso o certificado seja classificado como inválido.

1.9.18. Permitir filtros de URL customizados por políticas.

1.9.19. Permitir filtros de URL baseado em base de dados local.

1.9.20. Permitir controle de acesso a sites HTTP/HTTPS por meio de lista negra e lista branca armazenada localmente.

1.9.21. Permitir ou bloquear sites ou categorias de sites:

a) Por grupo do Active Directory.

b) Por Organization Unit (OU) do Active Directory.

c) Por faixa de tempo.

d) Por expressões de requisição URL.

e) Por domínio de URL.

1.9.22. Permitir o uso de expressões regulares para filtrar conteúdo existente no cabeçalho HTTP.

1.9.23. Suportar o controle de aplicações que trafeguem dados pela internet, permitindo monitoração e bloqueio das mesmas.

1.9.24. Suportar regras de exceção a tráfego SSL que não deve ser inspecionado

1.9.25. Suportar integração com solução de antivírus de gateway por meio do protocolo ICAP ou possuir a solução de antivírus incorporada no produto.

1.9.26. Suportar inspeção de conteúdo para verificação e eliminação de vírus e malwares.

1.9.27. Permitir a detecção de conteúdos maliciosos, suspeitos ou de atividades indesejadas por meio de análise comportamental do código, proporcionando proteção contra ameaças desconhecidas (Proteção Dia Zero).

1.9.28. Suportar análise de objetos encapsulados com a opção de bloqueio.

1.9.29. Suportar verificações de malware de forma concorrente para cada objeto analisado, em tempo real.

1.9.30. Verificar tráfego analisando os dados até a camada 7 do modelo OSI, identificando estações de trabalho da rede interna possivelmente infectadas por malwares.

1.9.31. Permitir identificar e bloquear aplicações maliciosas, inclusive dos tipos:

a) ActiveX.

b) Executáveis Windows.

c) Flash ActionScripts.

d) Java applets.

e) Java applications.

f) Java Scripts.

g) Potencialmente não desejados (spywares).

h) Visual Basic.

1.9.32. Permitir bloquear todos os comportamentos/técnicas abaixo:

a) Data theft: Backdoor.

b) Data theft: Keylogger.

c) Data theft: Password stealer.

d) Data theft: Spyware.

e) Detection evasion: Obfuscated code.

f) Detection evasion: Packed code.

g) Phishing (para webmail).

h) Potentially unwanted: Ad-/Spyware.

i) Potentially unwanted: Adware.

j) Potentially unwanted: Deceptive behavior.

k) Potentially unwanted: Dialer.

l) Potentially unwanted: Privacy violation.

m) Potentially unwanted: Redirector.

n) Potentially unwanted: Suspicious activity.

o) Stealth activity: Code injection.

p) Stealth activity: Rootkit.

q) System compromise: Browser exploit.

r) System compromise: Code execution exploit.

s) System compromise: Trojan downloader.

t) System compromise: Trojan dropper.

u) System compromise: Trojan proxy.

v) System compromise: Trojan.

w) Viral Replication: File infector vírus.

x) Viral Replication: Network worm.

y) Web threats: Cross-site scripting.

z) Web threats: Infected website.

aa) Web threats: Vulnerable ActiveX controls.

1.10. **Na função de balanceamento de carga:**

1.10.1. Permitir o balanceamento de no mínimo 5 servidores reais para um servidor virtual, de forma transparente aos usuários finais.

1.10.2. Permitir o uso dos seguintes métodos de balanceamento:

a) Estático.

b) Round-robin.

c) Baseado no menor round trip time.

1.10.3. Permitir o balanceamento de HTTP, HTTPS e SSL.

1.10.4. Permitir o balanceamento de serviços genéricos em camada 4 (TCP e UDP).

1.10.5. Permitir o balanceamento de protocolos IP genéricos em camada 3.

1.10.6. Permitir o balanceamento de tráfego entre dois links internet de duas operadoras distintas, realizando a monitoração da disponibilidade de cada link e, em caso de detecção de queda de um dos links internet, deve direcionar o tráfego para o outro link. Quando o link que falhou for restabelecido, deverá retomar o balanceamento pelos dois links.

1.11. **Na função de antivírus de Gateway:**

1.11.1. Permite a inspeção de tráfego em tempo real por vírus nos protocolos HTTP, SMTP.

1.11.2. Permite o bloqueio de download de arquivos por tipo.

1.11.3. Permite o bloqueio de download de arquivos maliciosos do tipo adware, spyware, hijackers, keyloggers, etc.

1.12. **Na função de prevenção de intrusão - IPS:**

1.12.1. Permitir a utilização de IPS inline protegendo no mínimo o mesmo número de interfaces definidas no item 1.7.1.

1.12.2. Permitir a detecção e proteção contra intrusão de hosts/redes.

1.12.3. Possuir a capacidade de remontar pacotes para identificação de ataques.

1.12.4. Suportar contenção de pelo menos os seguintes mecanismos de detecção e proteção de ataques:

a) Análise de protocolos.

b) Detecção de anomalias.

c) Detecção de ataques de RPC e MS-RPC.

d) Reconhecimento de padrões.

e) Proteção/bloqueio contra-ataques nos protocolos SMB v1, v2 e v2.1, SMTP, IMAP, POP, DNS, SYSLOG, SSL, FTP, SSH, ICMP, HTTP/HTTPS, PEER-2-PEER, H.225 SIP.

1.12.5. Possuir ao menos os seguintes métodos de notificação:

a) Registro na console de administração.

b) Alertas via correio eletrônico ou trap SNMP.

1.12.6. Possuir ao menos os seguintes métodos de resposta a ataques:

a) Armazenamento de log de sessão.

b) Inclusão de host/rede em lista negra.

c) Termino de sessões via reset de conexão TCP.

1.12.7. Permitir atualização automática das assinaturas para o sistema de detecção de intrusão.

1.12.8. Permitir a mitigação de efeitos de ataque de negação de serviço.

1.12.9. Permitir a filtragem de ataque por anomalia de tráfego.

1.12.10. Permitir filtragem de ataque de negação de serviço, reconhecimento, exploit e evasão de firewall.

1.12.11. Permitir filtragem de ataque na camada de aplicação.

1.12.12. Possuir throughput de inspeção de tráfego real de IPS de no mínimo 10 Gbps (dez gigabits por segundo).

1.12.13. Permitir implantação de identificação de intrusão (passivo) ou prevenção de intrusão (ativo) simultaneamente no mesmo equipamento, em regras para pares de redes ou hosts diferentes, mesmo as regras sejam aplicáveis as mesmas interfaces.

1.12.14. Permite inspeção utilizando técnicas de inspeção profunda de pacotes (DPI – Deep Packet Inspection) ou na modalidade Stateful Inspection.

1.12.15. Permite a detecção e prevenção de ataques não orientados à conexão.

1.12.16. Permite a execução de todas as funções de inspeção sem a instalação de agentes nos hosts a serem protegidos.

ITEM 2 - SOLUÇÃO DE PREVENÇÃO CONTRA ATAQUES AVANÇADOS

2.1. A solução para proteção contra ameaças avançadas deverá funcionar completamente integrada sendo capaz de receber arquivos, e-mails, URL's, dentro outros, para análise avançada.

2.2. A solução para proteção contra ameaças avançadas deverá ser capaz de:

2.2.1. Detectar ataques direcionados persistentes – APT.

2.2.2. Gerar índices de comprometimento bem como bloquear ameaças persistentes direcionadas ao órgão e ao serviço de e-mail do CONTRATANTE.

2.2.3. Realizar a análise virtual de ameaças.

2.2.4. Detectar conteúdo malicioso.

2.2.5. Analisar todos os estágios de uma sequência de ataques.

2.2.6. Proteger contra-ataques em rede.

2.2.7. Monitorar e gerir riscos que permitam a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente.

2.2.8. Detecção, visibilidade, bloqueio e informação sobre incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos.

2.2.9. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas.

2.2.10. Permitir a rápida identificação da criticidade dos eventos de segurança.

2.2.11. Permitir realizar pesquisas avançadas e customizadas das análises realizadas através da console de gerenciamento.

2.2.12. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de análises realizadas.

2.2.13. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento.

2.2.14. Permitir a integração com sistemas de serviço de diretório.

2.2.15. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP.

2.2.16. A análise de SMTP será realizada em uma solução separada do sensor de HTTP e demais protocolos.

2.2.17. A análise em SMTP será realizando de modo MTA (Inline)

2.2.18. A análise de e-mail em sandbox deverá ocorrer em arquivos Microsoft Office, PDF, arquivos compactados e executáveis do tipo PE.

2.2.19. A análise em sandbox será realizada on-premise.

2.2.20. Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques.

2.2.21. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP.

2.2.22. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso.

2.2.23. Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS.

2.2.24. Deve possuir a habilidade de detectar e analisar os protocolos HTTP, HTTPS, SMTP e as seguintes extensões: 7z, .ace, .apk, .arj, .bat, .bz2, .cab, .cmd, .dll, .doc, .docm, .docx, .dot, .dotm, .dotx, .exe, .gz, .htm, html,

.jar, .js, .kgb, .lnk, .lzh, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip.

2.2.25. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura.

2.2.26. Capacidade de oferecer informações para analise forense de artefatos suspeitos de serem maliciosos.

2.2.27. Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças.

2.2.28. Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets.

2.2.29. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF's, executáveis, PPT, DOC, XLS, ZIP e RAR.

2.2.30. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP.

2.2.31. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho.

2.2.32. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações.

2.2.33. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança.

2.2.34. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados).

2.2.35. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística.

2.2.36. Deve possuir foco em proteção contra APTs (Advanced Persistent Threats).

2.2.37. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero).

2.2.38. Deverá suportar a distribuição das inspeções de tráfego em diferentes sensores, possibilitando assim obter uma melhor performance.

2.2.39. Deverá permitir a análise especifica de eventos de segurança de computadores suspeitos de atividade maliciosa.

2.2.40. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único.

2.2.41. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução.

2.2.42. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução.

2.2.43. Deve ter capacidade de atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede

2.2.44. Deve possuir interface web ou cliente servidor para busca e investigação local de incidentes.

2.2.45. Deve possuir capacidade de envio de artefatos para analisador virtual dedicado, externo, sendo que este deverá suportar no mínimo os sistemas operacionais Windows 7 e Windows 10.

2.2.46. Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento.

2.2.47. Deve possuir capacidade de análise virtual de artefatos internamente.

2.2.48. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets.

2.2.49. Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming.

2.2.50. Deve possuir estatística do tráfego analisado.

2.2.51. Deve possuir indicadores de risco do ambiente.

2.2.52. Recomendações de Segurança

2.2.53. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação.

2.2.54. Deve possibilitar customização de Sandbox, permitindo ao cliente utilizar seu padrão de imagens e sistemas operacionais no módulo de análise.

2.2.55. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling.

2.2.56. Deve ser capaz de detectar e bloquear tentativas de scan de rede.

2.2.57. Deve ser capaz de detectar e bloquear propagação de malwares na rede.

2.2.58. Deve ser capaz de detectar e bloquear tentativas de brute-force.

2.2.59. Deve ser capaz de detectar e bloquear tentativas de fuga e roubo de informação.

2.2.60. Deve ser capaz de detectar e bloquear ameaças que se replicam na rede.

2.2.61. Deve ser capaz de detectar e bloquear exploits na rede.

2.2.62. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP ou endereço MAC, porta e protocolo.

2.2.63. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos.

2.2.64. A análise em sandbox poderá ser realizada em ambiente virtualizado ou em servidor bare-metal.

2.2.65. Deve suportar análise de documentos do Microsoft Office (DOC, DOCX, XLS, XLSX, PPT, PPTX).

2.2.66. Deve suportar análise de documentos em PDF.

2.2.67. Deve analisar dinamicamente arquivos compactados (ZIP, BZIP2, RAR).

2.2.68. Deve analisar dinamicamente binários PE de 32-bits.

2.2.69. Deve analisar dinamicamente bibliotecas dinâmicas (DLL).

2.2.70. Poder funcionar em ambiente totalmente virtualizado ou em appliance físico.

2.2.71. Deve possuir tecnologia própria de análise de artefatos em sandboxing.

2.2.72. Deve prover possibilidade de isolamento total da rede de sandbox da rede de gerência.

2.2.73. Deve prover possibilidade de uso da rede dedicada para a internet na análise de sandbox.

2.2.74. Deve analisar dinamicamente arquivos do Adobe Flash (SWF).

2.2.75. Deve realizar a análise localmente podendo ter consultas externas para reputação de IP e URL, mas sem envio da amostra.

2.2.76. Deve ter a capacidade de gerar relatórios com eventos realizados pela amostra no sistema alvo.

2.2.77. Deve analisar dinamicamente rootkits.

2.2.78. Caso uma ameaça baixe outra enquanto na sandbox, essa também deverá ser analisada num evento correlacionado.

2.2.79. Deve submeter uma amostra a sistemas operacionais diferentes, a fim de detectar ações específicas para um sistema.

2.2.80. Capacidade de integração via API com soluções terceiras.

2.2.81. O fabricante deverá disponibilizar acesso a base de dados externa que possibilite a pesquisa em base de reputação/ categorização abastecida por informações de outras análises em outros clientes. Este acesso deverá ser web, e deverá possuir referências e atalhos nos próprios relatórios e logs locais da solução.

2.3. Deverá ser capaz de identificar softwares ou comportamentos maliciosos, tais como:

2.3.1. Malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede.

2.3.2. Vermes de rede e de e-mail no tráfego de rede.

2.3.3. Programas de exploração de vulnerabilidades (Exploits) na rede.

2.3.4. Ataques de engenharia social que procurem fazer com que o usuário forneça suas credenciais de acesso (phishing, spear phishing).

2.3.5. Empacotamentos maliciosos no tráfego da rede.

2.3.6. Tráfego web malicioso através de consultas a sistemas de reputação na Internet.

2.3.7. Tentativas de roubo de informação.

2.3.8. Outros incidentes de segurança que representem risco a integridade, disponibilidade ou autenticidade de informação do CONTRATANTE.

2.4. Características de Desempenho e Escalabilidade:

2.4.1. Suportar uma análise de tráfego agregado de, no mínimo, 1 Gbps (um gigabit por segundo) e suportar a análise de, no mínimo, 10.000 (dez mil) arquivos por hora.

2.4.2. Ser capaz de processar, no mínimo, 200.000 (duzentos mil) mensagens por hora.

2.4.3. A solução deverá prover as funcionalidades de inspeção inbound de Malware com filtro de ameaças avançadas e análise de execução em tempo real, inspeção outbound de call-backs.

2.5. Características do Gerenciamento da Solução:

2.5.1. A console de gerenciamento deve informar origens georeferenciadas de ataques e eventos de segurança monitorados pela solução.

2.5.2. Implementar gerenciamento centralizado com no mínimo as seguintes funções: criação de regras de tratamento de malware, administração de usuários, configurações de host e network.

2.5.3. Implementar mecanismo de triangulação e correlação dos vetores de ataque.

2.5.4. Em caso de indisponibilidade da console de gerenciamento o restante da solução permaneça ativa e funcionando.

2.5.5. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e analise.

2.5.6. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração.

2.5.7. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização.

2.5.8. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas.

2.5.9. Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática.

2.5.10. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções.

2.5.11. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques.

2.5.12. Deverá possuir capacidade de identificar a origem de ataques direcionados, incluindo a análise de artefatos por meio de analisador virtual com a capacidade de gerar no mínimo 24 máquinas virtuais de análise.

2.5.13. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque.

2.5.14. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações:

a) Uso de CPU

b) Uso de Disco.

c) Uso de Memória.

d) Tráfego malicioso analisado.

e) Todo o tráfego analisado.

2.6. Características da Administração da Solução:

2.6.1. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS:

2.6.2. Implementar interface CLI segura através do protocolo SSH ou interface serial RS-232 ou similar.

2.6.3. Implementar base de usuários local e consulta a base de usuários externa através do protocolo LDAP.

2.6.4. Implementar sincronização de hora através de protocolo NTP.

2.6.5. Implementar no mínimo 02 (dois) níveis de administração distintos.

2.6.6. Implementar através da interface gráfica, seleção dos níveis e módulos de geração de log, tais como: log de autenticação, log de falhas de harware, log de eventos de sistema, log de atualização e log de mudança de configuração.

2.6.7. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc.

2.6.8. Implementar através da interface gráfica mecanismo de atualização da base de dados e de firmware da solução.

2.6.9. Implementar através da interface gráfica mecanismo de dashboard onde seja possível a visualização de no mínimo as seguintes informações: Sumário de detecção e proteção, gráfico de top infecções, e gráfico da quantidade de e-mails monitorados.

2.6.10. Implementar através da interface de administração, configuração de mecanismo de alerta onde seja possível configurar o modo de operação.

2.6.11. Implementar a atualização (updates) dos appliances via mecanismo de push ou automático dos seguintes módulos: segurança de conteúdo e atualização de patch.

2.6.12. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog ou protocolo proprietário do fabricante e deverá conter no mínimo:

a) Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware.

b) Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

2.6.13. A solução deverá ter integração com ferramentas de SIEM.

2.6.14. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa.

2.6.15. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor.

2.6.16. Deve trabalhar com geo-localização para identificar a origem geográfica de um ataque.

2.6.17. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado.

2.6.18. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar).

2.6.19. Deve permitir encaminhamento de logs via syslog.

2.6.20. Deve permitir a configuração de alarmes personalizados, com base em investigações.

2.6.21. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo:

a) Computadores infectados.

b) Origem de infecções.

c) Estatísticas de ameaças.

d) Eventos suspeitos.

e) Infecções de malware.

f) Capacidade de emitir relatórios baseados nas investigações.

g) Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos.

2.6.22. A solução deverá apresentar função de pesquisa por logs contendo no mínimo:

a) Critérios de pesquisa por dia, mês e ano.

b) Possibilidade de pesquisa pelo domínio ou conta, endereço IP e grupos.

c) Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção.

d) Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV.

ITEM 3 - SOLUÇÃO DE ARMAZENAMENTO DE LOGS

3.1. Deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

3.2. Permitir a visualização de match de regras através dos hit count ou hits de cada regra de firewall, controle de aplicação e filtro de urls.

3.3. Deve suportar acesso via SSH, cliente e WEB (HTTPS).

3.4. O gerenciamento deve permitir a monitoração de logs e ferramentas de investigação de logs.

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

3.6. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre.

3.7. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

3.8. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc.

3.9. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware e Sandbox), e URLs que passaram pela solução.

3.10. Deve ser possível exportar os logs em CSV.

3.11. Possibilitar rotação do log.

3.12. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

3.12.1. Resumo gráfico de aplicações utilizadas.

3.12.2. Principais aplicações por utilização de largura de banda.

3.12.3. Principais aplicações por taxa de transferência de bytes.

3.12.4. Principais hosts por número de ameaças identificadas.

3.12.5. 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-Malware), de rede vinculadas a este tráfego.

3.12.6. Deve permitir a criação de relatórios personalizados.

3.13. Gerar alertas automáticos via e-mail em PDF ou HTML.

3.14. Deve consolidar logs e relatórios de todos os dispositivos administrados.

3.15. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de leitura e escrita e somente leitura.

3.16. Deverá possuir mecanismo "Drill-Down" para navegação e análise dos logs em tempo real.

3.17. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.

3.18. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

3.19. Disponibilizar recursos interativos de navegação nos eventos informados.

3.20. A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes: visualizar quantidade de tráfego utilizado de aplicações e navegação, bem como gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada.

3.21. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos.

3.22. A solução deve permitir o controle de alterações de forma visual e através de relatórios.

3.23. A solução deve possuir processo automático, formal para o acompanhamento, aprovação e alterações de política de segurança.

3.24. A solução deve suportar notificação por e-mail acerca das instalações de políticas.

3.25. Deve permitir mais de um administrador conectado em modo gravação (read-write), bloqueando o acesso aos recursos utilizados por cada administrador para evitar sobreposição de tarefas.

3.26. Deve permitir a customização de dashboards da solução.

3.27. A solução deverá prover funcionalidade para apoiar nos processos internos de gerência de mudanças e gerência de configuração.

3.28. A solução deve prover a possibilidade de auditar todas as mudanças de políticas com relatório detalhado de cada alteração efetuada.

3.29. A solução deve permitir um fluxo de aprovação da alteração efetuada para possibilitar que somente alterações gerencialmente aprovadas poderão ser efetivamente aplicadas.

3.30. A solução deverá prover um relatório detalhado da alteração para que seja possível uma revisão da alteração antes da aprovação.

3.31. Possuir capacidade de retenção de logs por, no mínimo, 6 meses.

ITEM 4 - SOLUÇÃO DE GERENCIAMENTO

4.1. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede desde que não sejam software livre.

4.2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança.

4.3. Centralizar a administração de regras e políticas dos equipamentos de NGFW, usando uma única interface de gerenciamento.

4.4. Permitir a visualização de match de regras através dos hits count ou hits de cada regra de firewall, controle de aplicação e filtro de urls.

4.5. O gerenciamento da solução deve suportar acesso via SSH, cliente e WEB (HTTPS).

4.6. O gerenciamento deve permitir a criação e administração de políticas de firewall, controle de aplicação, políticas de IPS, anti-malware, políticas de filtro de URL e políticas de prevenção de malware desconhecido

4.7. Acesso concorrente de administradores.

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

4.9. Criação de regras que fiquem ativas em horário definido.

4.10. Criação de regras com data de expiração.

4.11. Backup das configurações e rollback de configuração para a última configuração salva.

4.12. Validação de regras antes da aplicação.

4.13. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing).

4.14. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre.

4.15. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração.

4.16. Toda a comunicação entre os equipamentos gerenciados deve ser feita via certificado digital.

4.17. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, antivírus e anti-malware), etc.

4.18. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware e Sandbox), e URLs que passaram pela solução.

4.19. Geração de, no mínimo, os seguintes relatórios: resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, 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-Malware), de rede vinculadas a este tráfego.

4.20. Deve permitir a criação de relatórios personalizados.

4.21. Gerar alertas automáticos via e-mail em PDF ou HTML.

4.22. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance físico deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível/homologado com/para VMware ESXi.

4.23. Deve consolidar relatórios de todos os dispositivos administrados.

4.24. Implementar comunicação entre gerência e equipamentos de proteção de rede de forma criptografada via certificado digital.

4.25. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de leitura e escrita e somente leitura.

4.26. Deverá possuir mecanismo "Drill-Down" para navegação e análise em tempo real.

4.27. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso.

4.28. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc.

4.29. Disponibilizar recursos interativos de navegação nos eventos informados.

4.30. A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

4.31. Visualizar quantidade de tráfego utilizado de aplicações e navegação.

4.32. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada.

4.33. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos.

4.34. A solução deve permitir o controle de alterações de forma visual e através de relatórios.

4.35. A solução deve possuir processo automático, formal para o acompanhamento, aprovação e alterações de política de segurança.

4.36. A solução deve permitir o gerenciamento de mudanças simplificado reduzindo os erros e poupando o tempo do administrador.

4.37. A solução deve suportar notificação por e-mail acerca das instalações de políticas.

4.38. A solução deve permitir revisão de alterações na ordem sequencial.

4.39. Deve permitir a customização de dashboards da solução de gerenciamento.

4.40. A solução deverá prover funcionalidade para apoiar nos processos internos de gerência de mudanças e gerência de configuração.

4.41. A solução deve permitir um fluxo de aprovação da alteração efetuada para possibilitar que somente alterações gerencialmente aprovadas poderão ser efetivamente aplicadas.

4.42. A solução deverá prover um relatório detalhado da alteração para que seja possível uma revisão da alteração antes da aprovação.

4.43. Deverá possuir ferramenta ou funcionalidade, que possa ser habilitada se desejado, que possibilite a um administrador submeter sugestão de modificação/inserção de regra e que a mesma só entre em produção após aprovação de um outro administrador ou gerente.

ITEM 5 - SOLUÇÃO DE SEGURANÇA MULTIFUNÇÃO PARA AMBIENTE VIRTUALIZADO

5.1. O sistema de proteção para segurança de máquinas virtuais deverá prover as seguintes funcionalidades já descritas nos itens anteriores: firewall, sistema de prevenção de intrusão – IPS, controle de aplicações, web filter, prevenção contra malwares e bots, prevenção contra ameaças avançadas de dia zero e inspeção de tráfego criptografado HTTPS.

5.2. O sistema de proteção deverá ser compatível com VMWare ESX 6.0 ou superior.

5.3. O sistema de proteção deverá ser compatível com VMWare NSX 6.1 ou superior

5.4. O sistema de proteção deverá possuir integração com o virtualizador em nível de hypervisor.

5.5. Permitir a replicação automatizada das configurações de segurança para as máquinas virtuais existentes e para as novas que foram criadas ou migradas.

5.6. Todas as proteções e funcionalidades deverão ser efetuadas sem a necessidade de instalação de agentes nas máquinas virtuais.

5.7. O sistema de proteção deve ser parceiro de tecnologia NSX da VMware.

5.8. O sistema de proteção deve ser automaticamente distribuído para os novos hosts ESX através da integração com NSX.

5.9. A solução deve suportar controle granular de políticas baseadas em grupos de segurança do NSX e objetos de máquinas virtuais do vCenter.

5.10. A solução deve suportar mecanismo de isolamento e remediação, informando ao NSX sobre uma máquina virtual infectada para que sejam tomadas ações preventivas.

5.11. A solução deve suportar gerenciamento centralizado e integrado tanto para os firewalls do ambiente virtualizado quanto para os firewalls físicos.

5.12. A solução deve possuir monitoramento e análise de logs e eventos centralizados, garantindo visibilidade e correlacionamento das ameaças.

5.13. A solução deve preservar nos logs os objetos conforme definidos no datacenter virtual, simplificando o monitoramento e análise do tráfego.

5.14. Permitir a criação de regras na console de gerenciamento centralizado utilizando os objetos diretamente da plataforma ESX e NSX.

5.15. Ser transparente garantindo as regras de segurança, sem necessidade de alteração na Gerência Centralizada de Segurança quando os endereços IP dos hosts e máquinas virtuais forem alterados nos hypervisors ESX e NSX.

LOTE 02

ITEM 1 – SOLUÇÃO DE FIREWALL DE APLICAÇÃO WEB

Os equipamentos, produtos, peças ou softwares necessários à Solução de Firewall de Aplicação deverão ser instalados no *datacenter* do CONTRATANTE, devendo observar os seguintes requisitos mínimos:

1.1. Deverá ser provida com emprego de 2 (dois) elementos com função de firewall de aplicação (WAF), para serem fixados em rack padrão 19".

1.2. Os componentes da solução integrada de segurança deverão ocupar no máximo 20U (Vinte Rack Units) de espaço no rack, considerando o somatório dos espaços utilizados por todos os componentes da solução.

1.3. Implementar cluster de alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo.

1.4. Possuir fontes de alimentação hot swappable 220v, redundantes N+1.

1.5. Cada um dos nós do cluster deve:

1.5.1. Possuir pelo menos 6 (seis) portas de comunicação dedicada, padrão Gigabit Ethernet (Cobre ou 1000Base-T SFP ou 1000Base-SX conector LC).

1.5.2. Deverão ser fornecidos 20 (vinte) patch cords CAT. 6 certificados, com comprimento de pelo menos 5 (cinco) metros, necessários a interligação das portas externas ao switch core do Datacenter.

1.5.3. Possuir porta independente para gerência, padrão Gigabit Ethernet (Cobre ou 1000Base-T SFP ou 1000Base-SX conector LC).

1.5.4. Possuir porta(s) independente(s) para sincronismo de cluster, padrão Gigabit Ethernet (Cobre ou 1000Base-T SFP ou 1000Base-SX conector LC).

1.6. Capacidade de inspecionar 2 Gbps (dois gigabits por segundo) de tráfego web em camada 7.

1.7. Admitir 50.000 (cinquenta mil) novas conexões por segundo para cada nó do cluster.

1.8. Admitir 10.000 (dez mil) transações por segundo (TPS) SSL com chaves RSA 2048 bits para cada nó do cluster.

1.9. Suportar 600.000 (seiscentos mil) conexões concorrentes.

1.10. Suportar agregação de portas (trunk).

1.11. Suportar o protocolo 802.1q.

1.12. Analisar tráfego HTTP/1.0, HTTP/1.1 e HTTP/2.0.

1.13. Restringir métodos HTTP/ HTTPS permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.

1.14. Permitir as seguintes opções de implementação:

1.14.1. Monitoramento (sem bloqueio).

1.14.2. Proxy (reverso e transparente).

1.15. Permitir que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento.

1.16. Remover as mensagens de erro do conteúdo que será enviado aos usuários.

1.17. Em modo "monitoramento" (sem bloqueio), realiza análise e avaliação do tráfego, gera relatórios com os dados analisados e simula bloqueios para efeito de avaliação.

1.18. Proteger contra-ataques automatizados, incluindo bots e web scraping, identificando comportamento não humano, navegadores operados por scripts ou qualquer outra forma que não operados por humanos.

1.19. Bloquear ataques aos servidores de aplicação, por meio dos seguintes recursos:

1.19.1. Identificação, isolamento e bloqueio de ataques sofisticados sem impactar nas transações das aplicações.

1.19.2. Identificação, isolamento e bloqueio de ataques sofisticados para os protocolos: HTTP e HTTPS.

1.19.3. Permitir a utilização de modelo positivo de segurança para proteger contra-ataques às aplicações HTTP e HTTPS, além de proteção contra-ataques conhecidos aos protocolos HTTP e HTTPS.

1.19.4. Quando detectada uma tentativa de ataque bloquear de imediato o tráfego ou a sessão.

1.19.5. Bloqueio com intermediação e interrupção da conexão.

1.19.6. Criação de políticas automáticas que bloqueiam o endereço IP que realizar violações.

1.19.7. Utilização de página HTML informativa e personalizável como HTTP Response aos bloqueios.

1.19.8. Configuração de políticas de bloqueio baseadas em requisição HTTP, endereço IP e usuário de aplicação.

1.20. Permitir apenas transações de aplicações validadas, o restante das transações deverá ser bloqueado, utilizando bloqueio por nível de aplicação baseado no contexto da sessão do usuário, com privilégios de autorização diferentes, entradas de usuários e tempo de resposta de aplicação.

1.21. Identificar e armazenar o ataque acontecido com detalhes, com as seguintes informações:

1.21.1. Cópia da tentativa do ataque.

1.21.2. Endereços IP que originaram os ataques.

1.21.3. Horário do ataque.

1.21.4. Nome do ataque.

1.21.5. Qual campo foi atacado.

1.21.6. Quantas vezes esse ataque foi realizado.

1.22. Armazenar informações de identificação dos usuários autenticados nas aplicações.

1.23. Suportar request compression e response compression.

1.24. Assinar cookies digitalmente e edita endereços de URL ("URL Rewriting").

1.25. Proteger as aplicações de banco de dados contra-ataques conhecidos.

1.26. Suportar aplicações que utilizam autenticação com estes métodos:

1.26.1. Autenticação básica.

1.26.2. NTLM.

1.26.3. Certificados SSL.

1.27. Possuir a capacidade de importar os certificados e pares de chaves pública/privada para as soluções que utilizam SSL para transferência de dados, atuando como man-in-the-middle para tráfego SSL.

1.28. Possuir mecanismo de aprendizado automatizado capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres, se é um campo obrigatório e ainda se é somente-leitura), cookies, arquivos XML, ações SOAP, e elementos XML.

1.29. Identificar e criar perfil de utilização dos aplicativos, inclusive desenvolvidos em Javascript, CGI, ASP e PHP.

1.30. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.

1.31. Correlaciona múltiplos eventos de segurança em conjunto para distinguir de forma precisa o tráfego permitido do tráfego malicioso.

1.32. Identifica ataques baseados em:

1.32.1. Assinaturas, com atualização diária da base pelo fabricante.

1.32.2. Regras.

1.32.3. Perfis de utilização.

1.33. Detectar ataques de força bruta por meio dos seguintes métodos:

1.33.1. Aumento do tempo de resposta da aplicação monitorada.

1.33.2. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP.

1.34. Detectar ataques do tipo força bruta em que:

1.34.1. O atacante solicita repetidamente o mesmo recurso.

1.34.2. O atacante realiza repetidas tentativas não autorizadas de acesso.

1.34.3. São utilizados ataques automatizados de login.

1.35. Detectar ataques do tipo força bruta que explorem:

1.35.1. Controles de acesso da aplicação (Erro 401 – Unauthorized).

1.35.2. Solicitações repetidas ao mesmo recurso, em qualquer parte/URL da aplicação.

1.35.3. Aplicações WEB que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação).

1.35.4. Gerenciamento de sessão (muitas sessões de um único endereço IP ou a um range de IPs).

1.35.5. Clientes automatizados (robôs, requisições muito rápidas).

1.36. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.

1.37. Possuir mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bidirecional atravessando o equipamento.

1.38. Possibilitar atualização de novas assinaturas para ataques conhecidos.

1.39. Apresentar proteção positiva e segura contra-ataques, como:

1.39.1. Anonymous Proxy Vulnerabilities.

1.39.2. Brute Force Login.

1.39.3. Buffer Overflow.

1.39.4. Cookie Injection.

1.39.5. Cookie Poisoning.

1.39.6. Cross Site Request Forgery (CSRF).

1.39.7. Cross Site Scripting (XSS).

1.39.8. Directory Traversal.

1.39.9. Forceful Browsing.

1.39.10. Form Field Tampering.

1.39.11. HTTP Denial of Service.

1.39.12. HTTP hidden field manipulation.

1.39.13. HTTP parameter pollution.

1.39.14. HTTP request smuggling.

1.39.15. HTTP Response Splitting.

1.39.16. HTTP Verb Tampering.

1.39.17. Illegal Encoding.

1.39.18. Known Worms.

1.39.19. LDAP injection.

1.39.20. Malicious Encoding.

1.39.21. Malicious Robots.

1.39.22. Parameter Tampering.

1.39.23. Remote File Inclusion Attacks.

1.39 24. Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI).

1.39 25. Session Hijacking.

1.39 26 Site Reconnaissance.

1.39.27. SQL Injection.

1.39.28. Web Scraping.

1.39.29. Web server software and operating system attacks.

1.39.30. Web Services (XML) attacks.

1.39.31. Zero Day Malware.

1.40. Permitir configurar granularmente, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.

1.41. Permitir definir regras de tamanho de arquivo para upload pelo método PUT.

1.42. A criação das políticas deve possuir as formas:

1.42.1. Automático por meio da observação do tráfego para a aplicação.

1.42.2. Automático por meio da observação do tráfego de teste e manual.

1.43. Suportar os seguintes critérios de decisão para realizar bloqueio ou gerar alerta, sendo que uma política pode conter um ou mais critérios simultaneamente:

1.43.1. Assinatura de ataque.

1.43.2 Código de response.

1.43.3. Conteúdo da cookie.

1.43.4. Conteúdo do cabeçalho.

1.43.5. Conteúdo do payload.

1.43.6. Horário.

1.43.7. Hostname.

1.43.8. IP de origem.

1.43.9. Método HTTP.

1.43.10. Número de ocorrências em determinado intervalo de tempo.

1.43.11. Parâmetro.

1.43.12. Tamanho da resposta de uma página web.

1.43.13. Tipo de protocolo (HTTP ou HTTPS).

1.43.14. User-agent (navegador).

1.43.15. Usuário.

1.44. Permitir a criação de assinaturas de ataques.

1.45. Reconhecer assinaturas seletivas, e filtros de ataque que devem proteger contra:

1.45.1. Ataques de negação de serviços automatizados.

1.45.2. Worms e vulnerabilidades conhecidas.

1.45.3. Requests em objetos restritos.

1.46. O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção a regra geral.

1.47. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação.

1.48. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos.

1.49. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual.

1.50. Possuir método de mitigação de DoS L7 baseado em:

1.50.1. Descarte de todas as requisições de um determinado IP e/ou país suspeito.

1.50.2. Geolocalização.

1.50.3. Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô.

1.51. Prevenir contra vazamentos dos códigos dos servidores.

1.52. Proteger contra as 10 maiores vulnerabilidades da lista OWASP.

1.53. Exportar requisições que contém os ataques, nos formatos PDF e CSV.

1.54. Realizar localização geográfica do IP, identificando pais de origem da requisição.

1.55. Aprender o comportamento da aplicação:

1.55.1. Campos, valores, cookies e URLs.

1.55.2. Políticas sugeridas somente devem ser aplicadas após um período configurável.

1.56. Inspecionar e monitorar até a camada de aplicação, todo tráfego de dados HTTP, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os requests e responses.

1.57. Realizar as checagens em todos os tipos de entrada de dados, como URLs, formulários, cookies, campos ocultos e parâmetros, consultas (query), métodos HTTP, elementos XML e ações SOAP.

1.58. Proteger contra mensagens XML e SOAP malformadas.

1.59. Utilizar o campo HTTP X-Forwarded-For sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com NAT.

1.60. Suportar SSL offload.

1.61. Remove as mensagens de erro do conteúdo que será enviado aos usuários.

1.62. Emitir os seguintes relatórios:

1.62.1. Gráfico indicando tipo de ataque.

1.62.2. Gráfico indicando tipo de violação.

1.62.3. Gráfico indicando quais URLs foram atacadas.

1.62.4. Gráfico indicando severidade.

1.62.5. Gráfico indicando os endereços IPs de origem.

1.62.6. Gráfico indicando a localização geográfica dos endereços IPs de origem.

1.63. Permitir a seleção de período para emissão dos relatórios, sendo que devem estar disponíveis os dados dos últimos 90 (noventa) dias.

1.64. Possuir console de administração com interface gráfica remota segura atendendo os seguintes requisitos:

1.64.1. Permitir a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e logs.

1.64.2. Permitir a replicação de configurações e a aplicação de atualização de softwares para os elementos dos nós do cluster.

1.64.3. Permitir a geração das seguintes informações, por período:

a) Permitir auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário.

b) Informações estatísticas de quantidade de conexões completadas e bloqueadas.

c) Informações estatísticas de fluxo de tráfego.

d) Informações estatísticas de quantidade de sessões ou conexões.

1.65. Permitir o balanceamento de aplicações em um pool de servidores, independentemente do hardware, sistema operacional e tipo de aplicação.

1.66. Suportar os seguintes métodos de balanceamento:

1.66.1. Round Robin.

1.66.2. Least Connection.

1.66.3. Por peso.

1.67. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.

1.68. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:

1.68.1. Por cookie.

1.68.2. Endereço de origem.

1.68.3. Sessão SSL.

1.68.4. Análise da URL acessada.

1.68.5. Através de qualquer parâmetro do cabeçalho HTTP.

1.69. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais: ICMP; TCP; HTTP, HTTPs.

1.70. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor.

1.71. Realizar Network Address Translation (NAT).

1.72. Realizar proteção contra syn flood.

1.73. Realizar as proteções de cabeçalho: X-Frame-Options, X-XSS-Protection, X-Content-Type-Options

1.74. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados seja realizada com aceleração em hardware, para não onerar o sistema.

1.75. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo "man in the middle", ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL sem comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.

1.76. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado.

1.77. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:

1.77.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS.

1.77.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS.

1.77.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea.

1.78. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS.

1.79. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

ATA DE REGISTRO DE PREÇOS N. 013/2017 - CJF

ANEXO II - RESUMO DO AMBIENTE TECNOLÓGICO DO CJF

1. Plataforma de Videoconferência

Equipamento/Software	Descrição	Quantidade
Sistema de Unidade de Controle Multiponto (MCU)	Marca Avaya; Modelo Scopia Elite 6110	1
Terminal de Comunicação FULLHD (1080p) CODEC	Marca Avaya; Modelo Scopia XT5000 + Scopia XT3WAY Microphone POD	4
Monitor LED	Marca Samsung; Modelo ED46D	8
Sistema de Acesso via PC e dispositivos móveis	Marca Avaya; Modelo Scopia Elite 6110 SFTW Licensing/PKG Scopia Management	10

2. Plataforma de Hardware

Tipo do Ativo	Marca/Modelo do Ativo	Descrição	Quantidade
Servidores Rack	IBM RISC pSeries p630 - 7028-6C4	4x 36GB HD, 12 GB de memória, 4 Processadores RISC Power4+, 1 Unidade fita DAT.	2
	DELL / PE R720	32 GB de memória, 2 x Quad Core Intel Xeon E5-2660	2
Servidores Blade	Chassis HP c7000	Cada chassi com 6 fontes	2
	HP / BL460C	Servidor de dois processadores de núcleo óctuplo com 256GB de RAM	23
Storages	NetApp FAS2040	2 Controladoras e uma capacidade de 40T bruto sendo 3 shelves com discos FC e SATA. Suporte para FCP, NFS, HTTP. Data-on-Tap 7.3.7	1
	NetApp FAS6290	2 Controladoras e uma capacidade de 200TB sendo 5 shelves com discos SATA e 5 shelves com discos SAS. Suporte para FCP, NFS, HTTP. Data-on-Tap 8.2	1
Tape Library (Biblioteca Robotizada)	QUANTUM / Scalar i500	Biblioteca composta por 4 drives LTO 5, com capacidade para 179 fitas LTO5, conexão via Fibre Channel	1
Escâner	Kodak i3400	Kodak i3400 com mesa digitalizadora padrão A3	5
Estações de trabalho	Dell Optiplex 7010	Desktop Core i7 8GB RAM 1TB	400

Tipo do Ativo	Marca/Modelo do Ativo	Descrição	Quantidade
		HDD	
	HP Elitebook 810	Notebook	17
Switches de Convergência	Cisco Nexus 5548UP	2 switches topo de rack com 48 portas sendo 16 FC de 8Gb/s e 32 Ethernet de 10Gb/s para rede local Storage/Blade	2
Switches de Core	H3C / S7506E	Concentradores da Rede Local 48 Portas Ethernet 10/100/1000 Mbps, 2 módulos de comunicação 10GB com 8 portas cada, 2 módulos Compat Flash com 2 portas 10GB	2
Switches de Acesso	H3C / S5500	Switchs ethernet 24 portas 10/100/1000 Mbps com Uplink 10Gbps e alimentação redundante	34
Controlador Rede Wireless	H3C / WX2200	Switch para Gerência Wireless com 3 portas	1
Access Points (APs)	H3C / AP3950	Acesso Rede Wireless 802.11a/b/g/n	40

3. Plataforma de Segurança

Tipo do Proteção	Marca / Modelo do Ativo	Descrição	Quantidade
Borda	Fortinet FortiGate 1500D	Firewall UTM com 4 portas 10 Gbps e 8 portas 1 Gbps	2
	Fortinet FortiWeb 3000D	Firewall de aplicação Web - WAF	2
E-mail	Trend Micro InterScan Messaging Security Virtual Appliance	Ferramenta de segurança de borda (MTA) para proteção anti-malware de e-mail	2
	Trend Micro ScanMail for Microsoft Exchange	Ferramenta de segurança para proteção anti-malware para Microsoft Exchange	2
Datacenter	Trend Micro Deep Security	Anti-malware para servidores de rede	400
Endpoint	Trend Micro OfficeScan	Anti-malware para estações de trabalho	500

Tipo do Proteção	Marca / Modelo do Ativo	Descrição	Quantidade
	Trend Micro Vulnerability Protection	Bloqueio contra exploração de vulnerabilidades conhecidas (virtual patch)	500
	Trend Micro Endpoint Application Control	Controle de aplicações instaladas nas estações de trabalho	500
Mobile	Trend Micro Mobile Security for Enterprise	Proteção para smartphones	10
Ferramentas de Gerência	Trend Micro Control Manager	Gerenciador dos produtos Trend Micro	1
	Trend Micro Smart Protection Server	Servidor de atualização e de verificação de reputação de arquivos que se comunica com a nuvem da Trend Micro	1
	Symantec Control Compliance Suite Vulnerabily Manager	Solução para gestão de vulnerabilidades de segurança dos ativos de TI	1
	Fortinet FortiAnalyzer 2000B	Centralizador de logs dos produtos Fortinet	1

4. Plataforma de Software

O quadro a seguir apresenta os sistemas operacionais, aplicativos, softwares de gerência, SGBDs, servidores de aplicação, servidores web e ferramentas em uso no CJF:

Software	Nome/Versão	Descrição
Sistema Operacional	MS / Windows 2003, 2008, 2008 R2 e 2012 Server	Sistema Operacional de 32 bits e 64 bits
	MS / Windows 7 Pro (Port) e Windows 10	Sistema Operacional de 64 bits
	Suse Linux 9,10, 11 e 12	Sistema Operacional de 32 bits e 64 bits
	IBM AIX 6.1	Sistema Operacional de 32 bits
	Oracle Linux 4/5/6/7	Sistema Operacional de 64 bits
	CentOS 4/5/6	Sistema Operacional de 32 bits e 64 bits

Software	Nome/Versão	Descrição
	Red Hat Linux 5, 6 e 7	Sistema Operacional de 32 bits e 64 bits
Servidores Aplicações	IIS 6.0 (Internet Information Services)	Servidor de Aplicações Microsoft ASP / HTML
	Apache 2.2.12	Servidor de Aplicações Apache / PHP
	Tomcat 5, 6 e 7	Servidor de Aplicações Java
	OAS 10g v10.1.35	Servidor de Aplicações Oracle
	Zope/Plone	Servidor de Aplicações Zope
	JBoss 5.1.0, EAP 6 e EAP 7	Servidor de Aplicações Jboss Java
Servidores Mensageria	Office365 – Skype (Lync)	Serviço em Nuvem
Servidores Correio Eletrônico	MS / Windows Exchange Server 2013	Serviço de correio eletrônico Exchange
Aplicativos	Office365 – 2013 e 2016	Suite de Aplicativos para Escritório
	IE 9 e 10, Chrome e Firefox	Software de Navegação Internet (Browser)
Softwares/Ferramentas de Gerência/Administração/Monitoração/Segurança	Webmin 1.350	Ferramenta de Administração de Servidores
	Zabbix 3.0	Software de Monitoramento do Ambiente
	VMware vSphere ESXi 6.0 U2	Ferramenta de Virtualização de Servidores
	Cacti 0.8.8b	Ferramenta de Estatística de Utilização de Rede
	Windows Media Services 9.0	Serviço de Streaming de Video
Gerenciador de Banco de Dados e ferramenta ETL	Postgres 9.1.3, 9.4	Sistema gerenciador de banco de dados Postgres
	MySql 5.0.26	Sistema gerenciador de banco de dados MySql
	SqlServer 2008	Sistema gerenciador de banco de dados SqlServer
	Ingres II 10.1	Sistema gerenciador de banco de dados Ingres

Software	Nome/Versão	Descrição
	Brs 8.0	Sistema gerenciador de banco de dados textual BRS
	Oracle 11g v11.2.03	Sistema gerenciador de banco de dados Oracle
	ODI 10 / Sunopsis	Ferramentas ETL Oracle Data Integrator e Sunopsis
Solução de Gerenciamento de Identidades e Controle de Acesso	Novell Identity Manager 2.7 Novell Access Manager 2.6.0 Novell iManager 2.7.0 Provisioning Module for Novell Identity Manager 2.7 Microsoft Active Directory 2008	Solução de Gerenciamento de Identidades e Controle de Acesso
Servidores Web	Mailman 2.1.15	Servidor de Listas de Discussão
	IMAP 4.1.3	Servidor de POP IMAP Courier
	PostFix 2.4.3	Servidor de SMTP
	Open LDAP	Servidor de Diretórios

5. CERTIFICAÇÃO DIGITAL

5.1. Certificado Digital Padrão ACJUS da cadeia ICP-Brasil.

ATA DE REGISTRO DE PREÇOS N. 013/2017 - CJF

ANEXO III - CRONOGRAMA DE IMPLANTAÇÃO

Prazo Máximo (em dias corridos)	Cronograma de Atividades da Prestação dos Serviços	Responsável
D	Data de emissão de Ordem de Serviço – OS dos equipamentos, softwares e serviços da solução pelo CONTRATANTE.	CJF
D + 3	Reunião de Planejamento.	CJF e CONTRATADA
D + 15	Entregar o Plano de Implantação contendo o planejamento das atividades para as etapas de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução.	CONTRATADA
D + 15	Comprovar que os técnicos que executarão as atividades são certificados pelos fabricantes dos componentes da solução.	CONTRATADA
	Aprovar o Plano de Implantação para as etapas de entrega, instalação, configuração e testes dos equipamentos e softwares que compõe a solução.	CJF
D + 45	Concluir a entrega dos equipamentos, softwares e acessórios, juntamente com toda a documentação técnica em meio eletrônico, completa e atualizada, contendo os manuais e guias de utilização e os demais documentos.	CONTRATADA
	Emitir o **Termo de Recebimento Provisório (TRP)** após a entrega dos equipamentos, softwares, Plano de Implantação aprovado e demais documentações da solução. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE. O recebimento provisório realizar-se-á no prazo máximo de 15 (quinze) dias corridos, contados da comunicação da empresa, desde que não haja pendências a cargo da CONTRATADA.	CJF
Data de Emissão do TRP + 15	Concluir, a partir da data de emissão do Termo de Recebimento Provisório (TRP), os serviços de instalação e configuração dos equipamentos e softwares da solução integrada de segurança, realizando todas as atividades programadas para esta etapa.	CONTRATADA
	Emitir o **Termo de Recebimento Definitivo (TRD)** após a finalização dos serviços de instalação e configuração, acompanhado da documentação técnica detalhada de todos os procedimentos executados, desde que não haja pendências a cargo da CONTRATADA.	CJF
Data de Emissão do TRP + 30	Realizar o acompanhamento ON-SITE da operação inicial da solução integrada de segurança, esclarecendo dúvidas e realizando ajustes na configuração visando à melhor utilização dos recursos oferecidos nos equipamentos que compõe a solução.	CONTRATADA

ATA DE REGISTRO DE PREÇOS N. 013/2017 - CJF

ANEXO IV – PLANILHA DE PREÇOS

LOTE 01				
Item	**Descrição**	**Qtde**	**Unitário**	**Total**
1	Solução em cluster de Gerenciamento Unificado de Ameaças (UTM).	1	R$ 625.000,00	R$ 625.000,00
1.1	Serviço de Instalação e configuração da solução.	1	R$ 1.000,00	R$ 1.000,00
1.2	Serviço de Suporte Técnico (mensal).	60	R$ 1.400,00	R$ 84.000,00
2	Solução de Prevenção contra-Ataques Avançados (APT).	1	R$ 1.060.000,00	R$ 1.060.000,00
2.1	Serviço de Instalação e configuração da solução.	1	R$ 36.000,00	R$ 36.000,00
2.2	Serviço de Suporte Técnico (mensal).	60	R$ 1.400,00	R$ 84.000,00
3	Solução de Armazenamento de Logs.	1	R$ 155.000,00	R$ 155.000,00
3.1	Serviço de Instalação e configuração da solução.	1	R$ 20.000,00	R$ 20.000,00
3.2	**Serviço de Suporte Técnico (mensal).**	**60**	**R$ 750,00**	**R$ 45.000,00**
4	Solução de Gerenciamento.	1	R$ 114.000,00	R$ 114.000,00
4.1	Serviço de Instalação e configuração da solução.	1	R$ 20.000,00	R$ 20.000,00
4.2	**Serviço de Suporte Técnico (mensal).**	**60**	**R$ 750,00**	**R$ 45.000,00**
5	Solução de Segurança Multifunção para Ambiente Virtualizado	18 hosts - 36 sockets	R$ 65.000,00	R$ 1.170.000,00
5.1	Serviço de Instalação e configuração da solução.	1	R$ 38.400,00	R$ 38.400,00
5.2	**Serviço de Suporte Técnico (mensal)**	**60**	**R$ 1.400,00**	**R$ 84.000,00**
6	Transferência de Conhecimento (por pessoa).	2	R$ 16.000,00	R$ 32.000,00
			Total Lote 01	**R$ 3.613.400,00**

LOTE 02				
Item	**Descrição**	**Qtde**	**Unitário**	**Total**
1	Solução em cluster de Firewall de Aplicação Web (WAF) com throughput de 2 Gbps.	1	R$ 754.000,00	R$ 754.000,00
2	Serviço de Instalação e configuração da solução.	1	R$ 40.000,00	R$ 40.000,00
3	**Serviço de Suporte Técnico (mensal).**	**60**	**R$ 1.600,00**	**R$ 96.000,00**
4	Transferência de Conhecimento (por pessoa).	2	R$ 9.000,00	R$ 18.000,00
			Total Lote 02	**R$ 908.000,00**

Total da Ata	**R$ 4.521.400,00**

ATA DE REGISTRO DE PREÇOS N. 013/2017 - CJF

ANEXO VII – TERMO DE CONFIDENCIALIDADE E SIGILO DA CONTRATADA

1. A empresa **NCT INFORMÁTICA LTDA,** pessoa jurídica com sede no SBS, Quadra 02, Lote 03, Bloco Q, 8º Andar, Sala 801, Centro Empresarial João Carlos Saad, Brasília-DF, CEP: 70.070-120], inscrita no CNPJ/MF com o n. 03.017.428/0001-35, neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente **EMPRESA RECEPTORA**, por tomar conhecimento de informações sobre o ambiente computacional do **CONSELHO DA JUSTIÇA FEDERAL – CJF**, aceita as regras, condições e obrigações constantes do presente Termo.

2. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do CONSELHO DA JUSTIÇA FEDERAL reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do contrato n. 24/2017.

3. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, pen drives, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, entre outros.

4. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do CONSELHO DA JUSTIÇA FEDERAL, das informações restritas reveladas.

5. A EMPRESA RECEPTORA compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao CONSELHO DA JUSTIÇA FEDERAL, as informações restritas reveladas.

6. A EMPRESA RECEPTORA deverá cuidar para que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao CONSELHO DA JUSTIÇA FEDERAL, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

7. A EMPRESA RECEPTORA possuirá ou firmará acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo.

8. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao CONSELHO DA JUSTIÇA FEDERAL qualquer violação das regras de sigilo estabelecidas neste Termo que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

9. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do CONSELHO DA JUSTIÇA FEDERAL, possibilitará a imediata rescisão de qualquer contrato firmado entre o CONSELHO DA JUSTIÇA FEDERAL e a EMPRESA RECEPTORA sem qualquer ônus para o CONSELHO DA JUSTIÇA FEDERAL. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, além das multas definidas no Termo de Referência, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONSELHO DA JUSTIÇA FEDERAL, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

10. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do CONSELHO DA JUSTIÇA FEDERAL.

11. E, por aceitar todas as condições e as obrigações constantes do presente Termo, a EMPRESA RECEPTORA assina o presente termo através de seus representantes legais.

Brasília - DF, 28 de dezembro de 2017.

Juiz Federal CLEBERSON JOSÉ ROCHA
Secretário-Geral, respondendo pela
Diretoria-Geral do Conselho da Justiça Federal

PRISCILA KIN YAMAMOTO JORANHEZON
Sócia-Administradora da empresa
NCT Informática Ltda