TRIBUNAL DE CONTAS DA UNIÃO
SECRETARIA DE LICITAÇÕES, CONTRATOS E PATRIMÔNIO
DIRETORIA DE LICITAÇÕES

EDITAL DO PREGÃO ELETRÔNICO Nº 086/2011

O **Tribunal de Contas da União - TCU** e este **Pregoeiro**, designado pela Portaria Segedam n.º 10, de 06 de janeiro de 2011, levam ao conhecimento dos interessados que, na forma da **Lei n.º 10.520/2002,** do **Decreto n.º 5.450/2005**, do **Decreto n.º 7.174/2010,** da **Lei Complementar n.º 123/2006** e, subsidiariamente, da **Lei n.º 8.666/1993** e de outras normas aplicáveis ao objeto deste certame, farão realizar licitação na modalidade **Pregão Eletrônico** mediante as condições estabelecidas neste Edital.

DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO:

DIA: 12 de dezembro de 2011
HORÁRIO: 10h (horário de Brasília/DF)
ENDEREÇO ELETRÔNICO: www.comprasnet.gov.br
CÓDIGO UASG: 30001

SEÇÃO I - DO OBJETO

1. A presente licitação tem como objeto o fornecimento de Solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; gestão de vulnerabilidades da rede TCU; resposta a incidentes de segurança e transferência de conhecimento para a equipe do Tribunal, conforme detalhamento constante no Anexo II – Especificações Técnicas deste Edital.

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

SEÇÃO II - DA DESPESA E DOS RECURSOS ORÇAMENTÁRIOS

2. A despesa total com a execução do objeto desta licitação é estimada em R$ 15.859.636,12 (quinze milhões oitocentos e cinquenta e nove mil seiscentos e trinta e seis reais e doze centavos), para o período de até 60 (sessenta) meses, conforme orçamento estimativo constante do Anexo I – Termo de Referência.

SEÇÃO III - DA PARTICIPAÇÃO NA LICITAÇÃO

3. Poderão participar deste **Pregão** os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - Sicaf e perante o

sistema eletrônico provido pela Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI), por meio do sítio www.comprasnet.gov.br.

3.1. Para ter acesso ao sistema eletrônico, os interessados em participar deste **Pregão** deverão dispor de chave de identificação e senha pessoal, obtidas junto à SLTI, onde também deverão informar-se a respeito do seu funcionamento e regulamento e receber instruções detalhadas para sua correta utilização;

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

4. Não poderão participar deste **Pregão:**

4.1. empresário suspenso de participar de licitação e impedido de contratar com o TCU, durante o prazo da sanção aplicada;

4.2. empresário declarado inidôneo para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação;

4.3. empresário impedido de licitar e contratar com a União, durante o prazo da sanção aplicada;

4.4. sociedade estrangeira não autorizada a funcionar no País;

4.5. empresário cujo estatuto ou contrato social não inclua o objeto deste **Pregão;**

4.6. empresário que se encontre em processo de dissolução, recuperação judicial, recuperação extrajudicial, falência, concordata, fusão, cisão, ou incorporação;

4.7. sociedades integrantes de um mesmo grupo econômico, assim entendidas aquelas que tenham diretores, sócios ou representantes legais comuns, ou que utilizem recursos materiais, tecnológicos ou humanos em comum, exceto se demonstrado que não agem representando interesse econômico em comum;

4.8. consórcio de empresa, qualquer que seja sua forma de constituição.

SEÇÃO IV - DA VISTORIA

5. O **licitante** deverá vistoriar as dependências do *datacenter* principal do TCU, em Brasília-DF, com o objetivo de inteirar-se das condições e grau de dificuldade existentes, mediante agendamento prévio de até 4 (quatro) dias úteis antes da data marcada para a sessão de abertura deste **Pregão**, junto à Serviço de Segurança em Tecnologia da Informação – Sesti, do Tribunal de Contas da União, por meio dos telefones (61) 3316-5499/3316-2489, conforme detalhado no Anexo I – Termo de Referência.

5.1. A vistoria será acompanhada por representante do TCU, designado para esse fim, o qual receberá o Termo de Confidencialidade e Sigilo do Licitante e visará a declaração comprobatória da vistoria efetuada, que deverão ter sido previamente elaborados e assinados, aonde pertinente, pelo **licitante** em conformidade com os modelos anexos a este Edital.

5.2. A pessoa a realizar a vistoria deve ser formalmente designada para tal fim pelo **licitante**, por meio de instrumento próprio, assinado por representante legal.

SEÇÃO V - DA PROPOSTA

6. O **licitante** deverá encaminhar proposta, exclusivamente por meio do sistema eletrônico, até a data e horário marcados para abertura da sessão , quando então encerrar-se-á automaticamente a fase de recebimento de propostas.

6.1. O **licitante** deverá consignar, na forma expressa no sistema eletrônico, o valor ofertado para cada item que compõe os grupos, já considerados e inclusos todos os tributos, fretes, tarifas e demais despesas decorrentes da execução do objeto.

6.2. O **licitante** deverá declarar, em campo próprio do sistema eletrônico, que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do Edital.

6.3. O **licitante** deverá declarar, em campo próprio do Sistema, sob pena de inabilitação, que não emprega menores de dezoito anos em trabalho noturno, perigoso ou insalubre, nem menores de dezesseis anos em qualquer trabalho, salvo na condição de aprendiz, a partir dos quatorze anos.

6.4. O **licitante** enquadrado como microempresa ou empresa de pequeno porte deverá declarar, em campo próprio do Sistema, que atende aos requisitos do art. 3º da LC n.º 123/2006, para fazer jus aos benefícios previstos nessa lei.

6.5. A declaração falsa relativa ao cumprimento dos requisitos de habilitação, à conformidade da proposta ou ao enquadramento como microempresa ou empresa de pequeno porte sujeitará o **licitante** às sanções previstas neste Edital.

7. As propostas ficarão disponíveis no sistema eletrônico.

7.1. Qualquer elemento que possa identificar o **licitante** importa desclassificação da proposta, sem prejuízo das sanções previstas nesse Edital.

7.2. Até a abertura da sessão, o **licitante** poderá retirar ou substituir a proposta anteriormente encaminhada.

8. As propostas terão validade de **60 (sessenta) dias**, contados da data de abertura da sessão pública estabelecida no preâmbulo deste Edital.

8.1. Decorrido o prazo de validade das propostas, sem convocação para assinatura do Contrato, ficam os **licitantes** liberados dos compromissos assumidos.

SEÇÃO VI - DA ABERTURA DA SESSÃO PÚBLICA

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

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

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

SEÇÃO VII - DA CLASSIFICAÇÃO DAS PROPOSTAS

12. O **Pregoeiro** verificará as propostas apresentadas e desclassificará, motivadamente, aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital.

13. Somente os **licitantes** com propostas classificadas participarão da fase de lances.

SEÇÃO VIII - DA FORMULAÇÃO DE LANCES

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

15. O **licitante** somente poderá oferecer lance inferior ao último por ele ofertado e registrado no sistema.

16. Durante o transcurso da sessão, os **licitantes** serão informados, em tempo real, do valor do menor lance registrado, mantendo-se em sigilo a identificação do ofertante.

17. Em caso de empate, prevalecerá o lance recebido e registrado primeiro.

18. Os lances apresentados e levados em consideração para efeito de julgamento serão de exclusiva e total responsabilidade do **licitante**, não lhe cabendo o direito de pleitear qualquer alteração.

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

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

21. No caso de a desconexão do **Pregoeiro** persistir por tempo superior a 10 (dez) minutos, a sessão do **Pregão** será suspensa automaticamente e terá reinício somente após comunicação expressa aos participantes no sítio www.comprasnet.gov.br.

22. O encerramento da etapa de lances será decidido pelo **Pregoeiro**, que informará, com antecedência de 1 a 60 minutos, o prazo para início do tempo de iminência.

23. Decorrido o prazo fixado pelo **Pregoeiro**, o sistema eletrônico encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá período de tempo de até 30 (trinta) minutos, aleatoriamente determinado pelo sistema, findo o qual será automaticamente encerrada a fase de lances.

SEÇÃO IX - DO BENEFÍCIO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

24. Após a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte, e houver proposta de microempresa ou empresa de pequeno porte que seja igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, proceder-se-á da seguinte forma:

24.1. A microempresa ou a empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos, apresentar proposta de preço inferior à do **licitante** mais bem classificado e, se atendidas as exigências deste Edital, ser contratada;

24.2. Não sendo contratada a microempresa ou empresa de pequeno porte mais bem classificada, na forma da subcondição anterior, e havendo outros **licitantes** que se enquadram na condição prevista no caput, estes serão convocados, na ordem classificatória, para o exercício do mesmo direito;

24.3. O convocado que não apresentar proposta dentro do prazo de 5 (cinco) minutos, controlados pelo Sistema, decairá do direito previsto nos artigos 44 e 45 da Lei Complementar nº 123/2006;

24.4. Na hipótese de não-contratação nos termos previstos nesta seção, o procedimento licitatório prossegue com os demais **licitantes**.

SEÇÃO X – DO DIREITO DE PREFERÊNCIA

25. Este **Pregão** submete-se às regras relativas ao direito de preferência estabelecidas no Decreto n.º 7.174/2010.

SEÇÃO XI - DA NEGOCIAÇÃO

26. O **Pregoeiro** poderá encaminhar contraproposta diretamente ao **licitante** que tenha apresentado o lance mais vantajoso, observado o critério de julgamento e o valor estimado para a contratação.

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

SEÇÃO XII - DA ACEITABILIDADE DA PROPOSTA

27. O **licitante classificado provisoriamente em primeiro lugar** deverá encaminhar a proposta de preço adequada ao último lance, em arquivo único, no prazo de 3 (três) horas, contado da convocação efetuada pelo **Pregoeiro** por meio da opção "Enviar Anexo" no sistema Comprasnet, em arquivo único, a proposta de preço adequada ao último lance, conforme modelo constante no Anexo III – Modelo de Planilha de Proposta de Preços.

27.1. Os documentos remetidos por meio da opção "Enviar Anexo" do sistema Comprasnet poderão ser solicitados em original ou por cópia autenticada a qualquer momento, em prazo a ser estabelecido pelo **Pregoeiro.**

27.1.1. Os originais ou cópias autenticadas, caso sejam solicitados, deverão ser encaminhados ao Serviço de Pregão e Cotação Eletrônica do Tribunal de Contas da União, situado no Setor de Administração Federal Sul – SAFS, quadra 04, lote 1, Anexo I, sala 143, CEP 70042-900, Brasília-DF.

27.2. O **licitante** que abandonar o certame, deixando de enviar a documentação indicada nesta seção, será desclassificado e sujeitar-se-á às sanções previstas neste Edital.

28. O **Pregoeiro** examinará a proposta mais bem classificada quanto à compatibilidade do preço ofertado com o valor estimado e à compatibilidade da proposta com as especificações técnicas do objeto.

28.1. O **Pregoeiro** poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal do TCU ou, ainda, de pessoas físicas ou jurídicas estranhas a ele, para orientar sua decisão;

28.2. Não se considerará qualquer oferta de vantagem não prevista neste Edital, inclusive financiamentos subsidiados ou a fundo perdido;

28.3. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade do **licitante**, para os quais ele renuncie à parcela ou à totalidade de remuneração;

28.4. Não se admitirá propostas de preços cujos valores sejam superiores aos orçados pelo TCU, conforme tabela de aceitabilidade constante no Anexo I – Termo de Referência, bem como, valor superior ao global máximo estipulado.

28.4.1. Caso o **licitante** ofereça em sua proposta, valor superior ao estipulado para algum item, deverá apresentar justificativa detalhada, informando os motivos e os componentes de custo que levaram a oferta ao patamar referenciado.

28.4.2. Caso o **licitante** apresente valores inferiores aos expressos na coluna de valores de referência para exequibilidade, este deve comprovar a viabilidade da execução contratual da proposta, por meio de demonstrativo analítico de todos os custos e receitas envolvidas.

SEÇÃO XIII - DA DEMONSTRAÇÃO DOS SERVIÇOS

29. Não se exigirá demonstração dos serviços ofertados.

SEÇÃO XIV - DA HABILITAÇÃO

30. A habilitação dos **licitantes** será verificada por meio do Sicaf (habilitação parcial) e da documentação complementar especificada neste Edital.

31. Os **licitantes** que não atenderem às exigências de habilitação parcial no Sicaf deverão apresentar documentos que supram tais exigências.

32. Os **licitantes** deverão apresentar a seguinte documentação complementar:

32.1. comprovação de patrimônio líquido não inferior a 10% (dez por cento) do valor estimado da contratação, quando qualquer dos índices Liquidez Geral, Liquidez Corrente e Solvência Geral, informados pelo Sicaf, for igual ou inferior a 1;

32.2. atestado ou certidão de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove ter o **licitante** prestado ou estar prestando serviços compatíveis com o objeto da licitação;

32.2.1. Considerar-se-á compatível com o objeto da licitação a execução de serviços gerenciados de segurança e o provimento de serviços baseados em centro de operações de segurança, em regime 24x7x365, em que sejam ou tenham sido prestados serviços de acordo com as características abaixo:

a) Prestação de serviços de *SOC (Secutiry Operation Center)*, incluindo o monitoramento e tratamento de incidentes e a consolidação e correlação de eventos;

i. a quantidade de ativos monitorados deverá ser de, no mínimo, 300 ativos (~50% da quantidade exigida no Anexo II – Especificações Técnicas);

b) Prestação de serviços de Análise de Vulnerabilidades, incluindo o monitoramento e o tratamento das vulnerabilidades encontradas;

i. a quantidade de ativos monitorados deverá ser de, no mínimo, 300 ativos (~50% da quantidade exigida no Anexo II – Especificações Técnicas);

c) “Fornecimento e instalação de equipamentos” ou “prestação de serviços de suporte e assistência técnica” ou “prestação de serviços de manutenção” para:

i. Firewall, em redes com, pelo menos, 2.500 (dois mil e quinhentos) hosts (50% da quantidade exigida no Anexo II – Especificações Técnicas), e

ii. IPS, em redes com, pelo menos, 2.500 (dois mil e quinhentos) hosts (50% da quantidade exigida no Anexo II – Especificações Técnicas).

d) "Fornecimento e instalação de equipamentos" ou "prestação de serviços de suporte e assistência técnica" ou "prestação de serviços de manutenção" para uma das tecnologias abaixo:

i. Proxy/cache com filtro de conteúdo WEB em redes com, pelo menos, 2.500 (dois mil e quinhentos) hosts (50% da quantidade exigida no Anexo II – Especificações Técnicas) ou

ii. SMTP Antispam em redes com, pelo menos, 2.500 (duas mil e quinhentas) caixas postais (50% da quantidade exigida no Anexo II – Especificações Técnicas) ou

iii. Firewall de aplicação (WAF) em redes com, pelo menos, 2.500 (dois mil e quinhentos) hosts (50% da quantidade exigida no no Anexo II – Especificações Técnicas).

e) caso sejam utilizados produtos em regime de licenciamento *software* livre na solução fornecida, deve ser apresentado atestado de capacidade técnica comprovando ter o **licitante** fornecido (instalado e administrado) e prestado suporte técnico em redes com, pelo menos, 2.500 (dois mil e quinhentos) hosts.

32.2.2. Os serviços podem estar distribuídos em diversos atestados, não se exigindo que todos eles sejam prestados a um mesmo cliente, mas cada um deles deve ser prestado, ou ter sido prestado, para o quantitativo mínimo de ativos, *hosts* ou caixas postais, não sendo admitida a soma de atestados diferentes de forma a atingir tais quantitativos.

32.3. declaração de vistoria, conforme modelo constante do Anexo X.

33. O **Pregoeiro** poderá consultar sítios oficiais de órgãos e entidades emissores de certidões, para verificar as condições de habilitação dos **licitantes**.

34. Os documentos que não estejam contemplados no Sicaf deverão ser remetidos em conjunto com a proposta de preços indicada na Condição 27, em arquivo único, por meio da opção "Enviar Anexo" do sistema Comprasnet, em prazo idêntico ao estipulado na mencionada condição.

34.1. Os documentos remetidos por meio da opção "Enviar Anexo" do sistema Comprasnet poderão ser solicitados em original ou por cópia autenticada a qualquer momento, em prazo a ser estabelecido pelo **Pregoeiro.**

34.1.1. Os originais ou cópias autenticadas, caso sejam solicitados, deverão ser encaminhados ao Serviço de Pregão e Cotação Eletrônica do Tribunal de Contas da União, situado no Setor de Administração Federal Sul – SAFS, Quadra 04, Lote 1, Anexo I, sala 143, CEP 70042-900, Brasília-DF.

34.2. Sob pena de inabilitação, os documentos encaminhados deverão estar em nome do **licitante**, com indicação do número de inscrição no CNPJ;

34.3. Todos os documentos emitidos em língua estrangeira deverão ser entregues acompanhados da tradução para língua portuguesa, efetuada por tradutor juramentado, e também devidamente consularizados ou registrados no cartório de títulos e documentos;

34.4. Documentos de procedência estrangeira, mas emitidos em língua portuguesa, também deverão ser apresentados devidamente consularizados ou registrados em cartório de títulos e documentos;

34.5. Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz;

34.6. Em se tratando de microempresa ou empresa de pequeno porte, havendo alguma restrição na comprovação de regularidade fiscal, será assegurado o prazo de 2 (dois) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, prorrogáveis por igual período, a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do débito, emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa;

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

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

36. Constatado o atendimento às exigências fixadas neste Edital, o **licitante** será declarado vencedor.

SEÇÃO XV - DO RECURSO

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

37.1. A falta de manifestação no prazo estabelecido autoriza o **Pregoeiro** a adjudicar o objeto ao **licitante vencedor**;

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

37.3. O **licitante** que tiver sua intenção de recurso aceita deverá registrar as razões do recurso, em campo próprio do sistema, no prazo de 3 (três) dias, ficando os demais **licitantes**, desde logo, intimados a apresentar contrarrazões, também via sistema, em igual prazo, que começará a correr do término do prazo da recorrente;

37.4. Para efeito do disposto no § 5º do artigo 109 da Lei n.º 8.666/1993, ficam os autos franqueados aos interessados.

38. Para justificar sua intenção de recorrer e fundamentar suas razões ou contrarrazões de recurso, o **licitante** interessado poderá solicitar vista dos autos a partir do encerramento da fase de lances.

39. As intenções de recurso não admitidas e os recursos rejeitados pelo **Pregoeiro** serão apreciados pela autoridade competente.

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

SEÇÃO XVI - DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

42. A homologação deste **Pregão** compete ao Secretário-Geral de Administração do Tribunal de Contas da União.

43. O objeto deste **Pregão** será adjudicado globalmente ao **licitante** vencedor.

SEÇÃO XVII – DO INSTRUMENTO CONTRATUAL

44. Depois de homologado o resultado deste **Pregão**, o **licitante** vencedor será convocado para assinatura do contrato, dentro do prazo de 5 (cinco) dias úteis, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste edital.

44.1. Poderá ser acrescentada ao contrato a ser assinado qualquer vantagem apresentada pelo **licitante** vencedor em sua proposta, desde que seja pertinente e compatível com os termos deste edital.

45. O prazo para a assinatura do contrato poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo **licitante** vencedor durante o seu transcurso, desde que ocorra motivo justificado e aceito pelo TCU.

46. Por ocasião da assinatura do contrato, verificar-se-á por meio do Sicaf e de outros meios se o **licitante** vencedor mantém as condições de habilitação.

47. Quando o **licitante** convocado não assinar o contrato no prazo e nas condições estabelecidos, poderá ser convocado outro **licitante** para assinar o contrato, após negociações e verificação da adequação da proposta e das condições de habilitação, obedecida a ordem de classificação, conforme estabelece o § 2º do art. 64 da Lei 8.666/1993.

SEÇÃO XVIII - DAS SANÇÕES

48. O **licitante** será sancionado com o impedimento de licitar e contratar com a União e será descredenciado no Sicaf e no cadastro de fornecedores do TCU, pelo prazo de até 5 (cinco) anos, sem prejuízo de multa de até 30% (trinta por cento) do valor estimado para a contratação e demais cominações legais, nos seguintes casos:

48.1. cometer fraude fiscal;

48.2. apresentar documento falso;

48.3. fizer declaração falsa;

48.4. comportar-se de modo inidôneo;

48.5. não assinar o contrato no prazo estabelecido;

48.6. deixar de entregar a documentação exigida no certame;

48.7. não mantiver a proposta.

49. Para os fins da subcondição 48.4, reputar-se-ão inidôneos atos como os descritos nos artigos 90, 92, 93, 94, 95 e 97 da Lei n.º 8.666/93.

SEÇÃO XIX - DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

50. Até 2 (dois) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa, física ou jurídica, poderá impugnar o ato convocatório deste **Pregão** mediante petição a ser enviada exclusivamente para o endereço eletrônico cpl@tcu.gov.br.

51. O **Pregoeiro**, auxiliado pelo setor técnico competente, decidirá sobre a impugnação no prazo de 24 (vinte e quatro) horas.

52. Acolhida a impugnação contra este Edital, será designada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

53. Os pedidos de esclarecimentos devem ser enviados ao **Pregoeiro** até 3 (três) dias úteis antes da data fixada para abertura da sessão pública, exclusivamente para o endereço eletrônico cpl@tcu.gov.br.

54. As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no sistema eletrônico para os interessados.

SEÇÃO XX - DISPOSIÇÕES FINAIS

55. Ao Secretário-Geral de Administração do Tribunal de Contas da União compete anular este **Pregão** por ilegalidade, de ofício ou por provocação de qualquer pessoa, e revogar o certame por considerá-lo inoportuno ou inconveniente diante de fato superveniente, mediante ato escrito e fundamentado.

55.1. A anulação do **Pregão** induz à do contrato;

55.2. Os **licitantes** não terão direito à indenização em decorrência da anulação do procedimento licitatório, ressalvado o direito do contratada de boa-fé de ser ressarcido pelos encargos que tiver suportado no cumprimento do contrato.

56. É facultado ao **Pregoeiro** ou à autoridade superior, em qualquer fase deste **Pregão**, promover diligência destinada a esclarecer ou completar a instrução do processo, vedada a inclusão posterior de informação ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação.

57. No julgamento das propostas e na fase de habilitação, o **Pregoeiro** poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos e a sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de classificação e habilitação.

57.1. Caso os prazos definidos neste Edital não estejam expressamente indicados na proposta, eles serão considerados como aceitos para efeito de julgamento deste **Pregão**.

58. Os documentos eletrônicos produzidos com a utilização de processo de certificação disponibilizada pela ICP-Brasil, nos termos da Medida Provisória n.º 2.200-2, de 24 de agosto de 2001, serão recebidos e presumidos verdadeiros em relação aos signatários, dispensando-se o envio de documentos originais e cópias autenticadas em papel.

59. Aplicam-se às cooperativas enquadradas na situação do art. 34 da Lei n.º 11.488, de 15 de junho de 2007, todas as disposições relativas às microempresas e empresas de pequeno porte.

60. Em caso de divergência entre normas infralegais e as contidas neste Edital, prevalecerão as últimas.

61. Este **Pregão** poderá ter a data de abertura da sessão pública transferida por conveniência do TCU, sem prejuízo do disposto no art. 4, inciso V, da Lei n.º 10.520/2002.

SEÇÃO XXI - DOS ANEXOS

62. São partes integrantes deste Edital os seguintes anexos:

62.1. Anexo I – Termo de Referência;

62.2. Anexo II – Especificações Técnicas;

62.3. Anexo III – Modelo de Planilha de Proposta de Preços;

62.4. Anexo IV – Termo de Confidencialidade e Sigilo do Licitante;

62.5. Anexo V – Termo de Confidencialidade e Sigilo da Contratada;

62.6. Anexo VI – Modelo de Ordem de Serviço de Treinamento;

62.7. Anexo VII – Modelo de Recebimento de Serviços de Treinamento;

62.8. Anexo VIII – Modelo de Ordem de Serviço;

62.9. Anexo IX – Modelo de Termo de Recebimento de Serviços;

62.10. Anexo X – Modelo de Declaração de Vistoria;

62.11. Anexo XI – Modelo de Atestado (*ou Declaração)* de Capacidade Técnica;

62.12. Anexo XII – Minuta de Contrato;

62.13. Anexo XIII – Modelo de Carta de Fiança Bancária para Garantia de Execução Contratual.

SEÇÃO XXII - DO FORO

63. As questões decorrentes da execução deste Instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de Brasília/DF, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro, por mais privilegiado que seja, salvo nos casos previstos no art. 102, inciso I, alínea “d” da Constituição Federal.

Brasília 23 de novembro de 2011.

RENATO TEIXEIRA LEITE DE LA ROCQUE

Pregoeiro

ANEXO I – TERMO DE REFERÊNCIA

I. OBJETO

Fornecimento de Solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; gestão de vulnerabilidades da rede TCU; resposta a incidentes de segurança e transferência de conhecimento para a equipe do Tribunal.

II. ESCOPO DA SOLUÇÃO

A Solução Integrada de Serviços Gerenciados de Segurança é composta por 10 (dez) itens de serviços contínuos em tecnologia da informação e abrange todo o ambiente computacional do TCU, compreendendo os *datacenters* central e de contingência, localizados em Brasília, nas Secretarias de Controle Externo nos Estados e no Instituto Serzedello Correa. Também farão parte do escopo atividades relacionadas à transferência de conhecimento e aos serviços técnicos especializados, segundo os requisitos mínimos elencados no Anexo II - Especificações Técnicas do Edital do Pregão Eletrônico n.º 86/2011.

III. DA VISTORIA

A vistoria deverá ser realizada nos termos da Seção IV do Edital.

IV. DO ORÇAMENTO ESTIMADO

Tabela I: Orçamento Estimado

Item	Valor (R$)
1 a 10	15.223.050,32
11	57.223,25
12	251.184,00
Valor Total	**15.859.636,12**

Tabela II: Valores de aceitabilidade máximos e de referência para exequibilidade:

Item	Valor de referência para exequibilidade (R$)	Valor máximo (R$)
1	266.070,00	1.046.813,33
2	391.217,82	1.516.156,50
3	404.528,71	1.424.053,68
4	446.558,23	1.368.947,73

5	514.690,85	2.046.362,91
6	418.950,00	1.426.939,78
7	373.448,60	841.279,14
8	600.600,00	3.778.066,50
9	225.635,20	1.046.600,80
10	458.542,56	3.406.058,55
11.1	1.968,04	15.818,77
11.2	1.968,04	15.818,77
11.3	1.614,29	15.437,17
11.4	1.260,54	13.055,58
11.5	1.260,54	13.055,58
11.6	1.260,54	13.055,58
11.7	1.968,04	15.818,77
11.8	1.260,54	13.055,58
11.9	906,79	11.673,98
11.10	906,79	11.673,98
12	161.280,00	320.380,44

Observações:

Não deverão ser oferecidos preços com valores superiores aos expressos na coluna de valores máximos da tabela acima. Caso o licitante assim proceda, deverá apresentar, ainda durante a fase de habilitação do pregão, justificativa detalhada, informando os motivos e os componentes de custo que levaram a oferta ao patamar referenciado.

Caso o licitante apresente valores inferiores aos expressos na coluna de valores de referência para exequibilidade, este deve comprovar a viabilidade da execução contratual da proposta, ainda durante a fase de habilitação do pregão, por meio de demonstrativo analítico de todos os custos e receitas envolvidas.

Observe-se que o total dos preços máximos é de R$ 18.360.123,12 (dezoito milhões, trezentos e sessenta mil, cento e vinte e três reais e doze centavos). Esse valor não reflete o orçamento estimado para fins de adjudicação, que é inferior a esse montante, ou seja, R$ 15.859.636,12 (quinze milhões oitocentos e cinquenta e nove mil seiscentos e trinta e seis reais e doze centavos), conforme Tabela I.

V. UNIDADE RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

Secretaria de Infraestrutura de Tecnologia da Informação do Tribunal de Contas da União – Setic.

VI. UNIDADE RESPONSÁVEL PELO ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

Secretaria de Infraestrutura de Tecnologia da Informação do Tribunal de Contas da União – Setic.

ANEXO II – ESPECIFICAÇÕES TÉCNICAS

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

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

O modelo de prestação de serviços conterá, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo Tribunal, tais como abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas periodicamente pela contratada, tais como análise de vulnerabilidades de segurança do parque computacional do TCU e monitoração das ferramentas utilizadas nos serviços. Ademais, a prestação dos serviços englobará entregas que serão utilizadas, principalmente, para mensuração e verificação dos serviços realizados, tais como os relatórios de monitoramento e relatórios de resolução de problemas.

Em suma, o serviço objeto da contratação é subdividido conforme a Tabela 1 abaixo:

Tabela 1 – Serviços contínuos de segurança da informação objeto da contratação

Item	Descrição	Quantidade	Meses
1	Serviços de *Firewall* Central Externo	1	60
2	Serviços de *Firewall* e *VPN* Central Interno	1	60
3	Serviços de *Firewall* e *VPN* Remoto	29	56
4	Serviços de Prevenção de Intrusão Central	2	53
5	Serviços de *Proxy/cache* com filtro de conteúdo *WEB*	1	57
6	Serviços de *SMTP Antispam*	1	57
7	Serviços de *Firewall* de Aplicação	1	53
8	Serviços de Consolidação e Correlacionamento de Eventos	1	60
9	Serviços de Gestão de Vulnerabilidades	1	56
10	Serviços de Monitoração e Administração de Segurança	1	60
11	Treinamentos	**Quantidade**	
11.1	*Firewall* Central Externo	1	
11.2	*Firewall* e *VPN* Central Interno	1	
11.3	*Firewall* e *VPN* Remoto	1	
11.4	Prevenção de Intrusão Central	1	

11.5	*Proxy/cache* com filtro de conteúdo *WEB*	1
11.6	*SMTP Antispam*	1
11.7	*Firewall* de Aplicação	1
11.8	Consolidação e Correlacionamento de Eventos	1
11.9	Gestão de Vulnerabilidades	1
11.10	Monitoração e Administração de Segurança	1
12	Serviços Técnicos Especializados	1.600 horas

Os itens 1 e 2 referem-se, respectivamente, aos **Serviços de "*Firewall* Central Externo"** e **de "*Firewall* e *VPN* Central Interno"**, providos, cada um, por um *cluster* de, pelo menos, dois equipamentos, capazes de regular o tráfego de dados entre as distintas redes do Tribunal e impedir a transmissão e recepção de tráfego nocivo ou não autorizado de uma rede para outra. Os equipamentos deverão implementar tecnologias de filtro de pacotes *stateful inspection,* utilizando mecanismos de verificação de tráfego segundo tabela de estado de conexões.

O *cluster* interno deverá possuir número de interfaces e capacidade de processamento superiores ao *cluster* externo, vez que grande parte do tráfego de dados ocorre internamente entre as redes sob administração do Tribunal. Oportunamente, um dos elementos de cada *cluster* deverá ser migrado para o *datacenter* de contingência do Tribunal no TST, em Brasília, sem descaracterizar o *cluster* formado.

Além disso, os equipamentos do *cluster* interno deverão ser capazes de implementar recursos de criptografia para tunelamento em redes inseguras de comunicação, tal como a *Internet*, por meio de redes privadas virtuais (*VPN*), garantindo confidencialidade, autenticação e integridade necessárias para a segurança do tráfego de dados do Tribunal. O canal de comunicação de dados para a formação dos túneis *VPN* não faz parte do escopo dessa contratação e será disponibilizado pelo TCU posteriormente. De forma a validar as funcionalidades de VPN, a contratada deverá prover infraestrutura de acesso à *Internet,* por meio de redes 3G, durante o período de operação assistida.

O item 3 refere-se aos **Serviços de "*Firewall* e *VPN* Remoto"** a serem prestados nas Secretarias de Controle Externos do TCU nos Estados e no Instituto Serzedello Corrêa, totalizando 29 localidades, com até 200 estações de trabalho cada uma. Tais serviços serão responsáveis por proteger as redes locais contra acessos não autorizados, sobretudo aqueles oriundos de redes externas, de modo a garantir a disponibilidade e integridade das informações trafegadas na Rede TCU. Deverão ser compostos por elementos de mesmo fabricante, com suporte à gerência e administração centralizada. Além disso, deverão implementar as mesmas políticas de *VPN* que serão adotadas pelos serviços do item 2, de modo a assegurar conexões seguras por meio de tunelamento criptografado na rede *Internet*.

O item 4 destina-se à prestação dos **Serviços de "Prevenção de Intrusão Central"** do Tribunal, providos por equipamentos capazes de identificar, prevenir e bloquear tentativas de intrusão e atividades maliciosas de rede entre os diversos segmentos de rede do TCU em Brasília, incluindo o acesso à *Internet,* à rede *MPLS* e à rede de contingência *VPN*. Deverão, ainda, implementar tecnologias de detecção e bloqueio de intrusão por meio de assinaturas e por análise de comportamento, com topologia *IPS in-line* em modo *pass-through/fail-over*. Deverão ser capazes de interromper tráfego de rede que tenha potencial para causar danos às informações ou ainda o consumo desnecessário de recursos de rede. Serão alocados dois

conjuntos de equipamentos, com as mesmas características, para serem instalados, inicialmente no *datacenter* central, em Brasília. Ambos os conjuntos devem ter as suas configurações sincronizadas e, oportunamente, um deles deverá ser migrado para o *datacenter* de contingência do Tribunal no TST, em Brasília.

O item 5 refere-se aos **Serviços de "*Proxy/cache* com Filtro de Conteúdo *WEB*"** responsável pela liberação e bloqueio de acessos feitos pelos usuários da rede corporativa à *websites* e assemelhados, conforme política de acesso à *Internet* definida pelo TCU. O serviço será provido em *cluster* e deverá ter seus elementos instalados, inicialmente, no *datacenter* principal do TCU, em Brasília, devendo ser utilizadas tecnologias de balanceamento ativo-ativo ou de tolerância a falhas ativo-passivo. Oportunamente, um dos elementos que compõem o *cluster* deverá ser migrado para o *datacenter* de contingência do Tribunal no TST, em Brasília, sem descaracterizar o *cluster* formado. O serviço deverá prover tecnologias de *proxy* transparente e *cache*.

Os **Serviços de "*SMTP Antispam*"** deverão ser prestados segundo as especificações técnicas elencadas no item 6. Refere-se à solução de bloqueio de *e-mails* não solicitados pelos usuários do Tribunal, capazes de impactar a produtividade de seus colaboradores e degradar o desempenho dos sistemas e redes corporativas, além de potencialmente comprometer a segurança das informações por eles custodiadas. Consistirá em dois elementos instalados, inicialmente, no *datacenter* principal do TCU, em Brasília, devendo utilizar tecnologias de balanceamento ativo-ativo ou de tolerância a falhas ativo-passivo. Será admitida a configuração do balanceamento por meio de prioridades em registros do tipo *MX* no *DNS* do Tribunal. Oportunamente, um dos elementos que compõem o *cluster* deverá ser migrado para o *datacenter* de contingência do Tribunal no TST, em Brasília, sem descaracterizar o *cluster* formado. Este serviço deverá suportar funções de *relay SMTP* e *antispam*, dotado de tecnologias de filtro de reputação, bloqueio por listas negras e quarentena por usuário.

Os **Serviços de "*Firewall* de Aplicação",** descritos no item 7 serão responsáveis por monitorar e bloquear entrada, saída, solicitação de acesso e chamadas de sistema a aplicações disponibilizadas em servidores *WEB*, segundo diretrizes de segurança definidas em conjunto com o TCU. Tais serviços deverão ser prestados com uso de elementos capazes de operar na camada de aplicação como um *proxy*, de modo a inspecionar conteúdo do tráfego de aplicações e bloquear tentativas de intrusão, vírus, exploração de vulnerabilidades e comunicações mal formatadas. Consistirá em dois elementos instalados inicialmente no *datacenter* principal do TCU, em Brasília, devendo utilizar tecnologias de balanceamento ativo-ativo ou de tolerância a falhas ativo-passivo. Oportunamente, um dos elementos que compõem o *cluster* deverá ser migrado para o *datacenter* de contingência do Tribunal no TST, em Brasília, sem descaracterizar o *cluster* formado. Os ajustes necessários a eventuais alterações de faixas de endereçamento e demais configurações deverão ser mapeadas e documentadas para compor procedimento operacional para recuperação em caso de indisponibilidade ou perda de desempenho do *datacenter* principal.

O item 8 trata dos **Serviços de "Consolidação e Correlacionamento de Eventos"** responsáveis por coletar, armazenar, processar, monitorar e correlacionar *logs* de ativos e servidores de rede do Tribunal, bem como da própria solução de segurança fornecida, de modo a executar ações reativas e proativas, como envio de notificações e alertas aos administradores da rede do Tribunal e da própria contratada. Os elementos a serem monitorados englobarão

switches, roteadores, servidores de rede, servidores de aplicação e de banco de dados do Tribunal, além dos próprios equipamentos adotados na solução de segurança provida. Não fará parte do escopo dos serviços o monitoramento de *desktops*, estações de videoconferência, *laptops*, *smartphones*, dispositivos *wireless*, impressoras e equipamentos de controle de acesso de pessoas às instalações do TCU.

O item 9 consiste em **Serviços de "Gestão de Vulnerabilidades"** capazes de detectar, inventariar e avaliar vulnerabilidades encontradas nos sistemas e recursos de TI e na solução de segurança fornecida, especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas. Deverá englobar instalação de agentes e validação de conformidade por meio de monitoração periódica e por demanda, segundo as diretrizes de segurança a serem definidas em conjunto com o Tribunal.

Os **Serviços de "Monitoração e Administração de Segurança"** descritos no item 10 serão os responsáveis por gerenciar remotamente e administrar equipamentos e *softwares* componentes da solução de segurança fornecida, envolvendo identificação de eventos que podem comprometer a segurança dos serviços de TI do Tribunal, manutenção da infraestrutura de segurança atualizada, mapeamento e execução de processos de resposta a incidentes de segurança, suporte à solução de segurança, avaliação periódica de configurações, entre outros, sob regime 24x7 (vinte e quatro horas por dia, sete dias por semana). Deverão ser prestados por meio de 2 (dois) Centros de Operações de Segurança (*Security Operations Centers* - *SOC*), de modo que a indisponibilidade de um deles não comprometa os níveis de serviços contratadas.

O item 11 trata dos **Treinamentos** a serem prestados ao TCU com vistas à transferência de conhecimento, compreendendo as tecnologias envolvidas nos serviços contratadas, assim como capacitação nos produtos e *softwares* utilizados para atender aos requisitos destas especificações técnicas. As atividades de treinamento serão realizadas para até 10 (dez) servidores da equipe do TCU e deverão possuir carga horária diária máxima de 4 (quatro) horas.

O item 12 trata de **Serviços Técnicos Especializados** em segurança da informação, com métrica baseada em horas de serviço, compreendendo a execução de atividades de elaboração de pareceres e planos, análise de ambiente e de ativos, auditoria forense, mudança de endereço de unidades do TCU (aspectos de segurança) e alteração de arquitetura do ambiente computacional e da infraestrutura de segurança do TCU. Consiste em atividades a serem demandadas por meio da celebração prévia de ordens de serviço, com total de horas definido previamente, de comum acordo entre o TCU e a contratada, cujo pagamento será efetivado somente após entrega de relatório de prestação de serviços e recebimento por parte do Tribunal.

À exceção dos itens 1 e 2, em que o *cluster* formado deve funcionar no modo ativo-ativo, para todos os demais serviços que exigirem a alocação de equipamentos, produtos, peças ou *softwares* em modo *cluster*, ou seja, em alta disponibilidade, ficará facultado à contratada escolher qual a melhor modalidade para a configuração da solução, seja tecnologia de balanceamento ativo-ativo ou de tolerância a falhas ativo-passivo. Em todos os casos devem ser respeitadas as capacidades mínimas requeridas para os serviços a serem entregues e que, no momento de contingência, os produtos alocados suportem, sem degradação, todos os requisitos destas especificações técnicas e dentro dos limites especificados no tópico IV – Nível

Mínimo de Serviços. Além disso a contratada deverá alocar, sem ônus adicional ao TCU, toda a infraestrutura necessária ao perfeito funcionamento do *cluster*.

A migração dos elementos que compõem *clusters* e que, oportunamente, serão migrados para o *datacenter* de contingência do Tribunal no TST, será feita de forma gradual, devendo o licitante planejar a migração de qualquer um dos serviços de forma isolada, sem impactar nos demais serviços providos, à exceção dos serviços objeto dos itens 1, 2 e 4, que serão migrados em conjunto.

Todas as interfaces de rede alocadas, incluindo-se as de gerência, sincronismo e aquelas que serão utilizadas para conectar os ativos do Tribunal nos *datacenters* deverão ser providas com interface para cabeamento de rede *UTP* com conector *RJ-45* no padrão *100/1000Base-T Gigabit Ethernet*. Já nas Secretarias de Controle Externo nos Estados, as interfaces deverão ser do tipo *UTP* com conector *RJ-45* no padrão *100Base-TX Fast Ethernet* ou 100/1000*Base-T Gigabit Ethernet*. A utilização de fibra óptica somente será admitida na interligação entre os equipamentos e servidores que hospedam os *softwares* de propriedade da contratada, como no caso de *link* de acesso remoto, a serem conectados aos Centros de Operação de Segurança (*SOC*).

O tópico VII – Topologia Requerida – define as características de instalação no ambiente computacional do *datacenter* principal do TCU e das Secretarias de Controle Externo nos Estados, que deverão ser levadas em consideração no mapeamento e definição dos elementos que comportarão os serviços contratadas. A arquitetura da solução adotada para o *datacenter* de contingência localizado no TST, em Brasília, se assemelhará à arquitetura para o *datacenter* principal localizado no TCU, assim como a arquitetura para o Instituto Serzedello Correa, que é equivalente à de uma Secretaria de Controle Externo nos Estados.

O desenho da topologia será entregue no ato da vistoria prévia, mediante entrega de Termo de Confidencialidade e Sigilo do licitante devidamente assinado pelo representante legal da empresa, com firma reconhecida (conforme Anexo IV – Termo de Confidencialidade e Sigilo do licitante) do Edital do Pregão Eletrônico n.º 86/2011.

I. ESPECIFICAÇÕES TÉCNICAS MÍNIMAS

São apresentadas, a seguir, especificações técnicas mínimas dos serviços a serem ofertados referentes aos itens 1 a 12 do objeto. Os termos “possui”, “permite”, “suporta” e “é” implicam no fornecimento de todos os elementos necessários à adoção da tecnologia ou funcionalidade citada. O termo “ou” implica que a especificação técnica mínima dos serviços pode ser atendida por somente uma das opções. O termo “e” implica que a especificação técnica mínima dos serviços deve ser atendida englobando todas as opções.

Todos os equipamentos, produtos, peças ou *softwares* necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de *end-of-sale*, *end-of-support* ou *end-of-life* do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Já os *softwares* comerciais deverão, ainda, ser instalados em sua versão mais atualizada, e estar cobertos por contratos de suporte a atualização de versão do fabricante durante toda a vigência do respectivo serviço. Da mesma maneira, todo o

hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante.

O conjunto dos requisitos especificados em cada item poderá ser atendido por meio de composição com os outros equipamentos, produtos, peças ou *softwares* utilizados no atendimento aos demais itens, desde que isso não implique em alteração da topologia ou na exposição de ativos a riscos de segurança.

Ademais, todos os componentes necessários à prestação dos serviços deverão ser compatíveis entre si, sem restrições aos requisitos constantes nestas especificações técnicas, e aos elencados do parque computacional do TCU.

1. Serviços de *Firewall* Central Externo:

Quantidade: 1

Meses de Prestação: 60 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de *Firewall* Central Externo** deverão ser instalados no *datacenter* principal e no *datacenter* de contingência do TCU, ambos em Brasília. Deverão proteger segmentos distribuídos nas redes externa e *DMZ*, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

1.1. providos com emprego de 2 (dois) elementos com função de *firewall* para serem fixados em *rack* padrão 19", sendo que o conjunto dos requisitos especificados poderão ser atendidos por meio de outros equipamentos, produtos, peças ou *softwares;*

1.2. implementa alta disponibilidade com tolerância a falhas, sendo admitida apenas a configuração ativo-ativo;

1.3. inicialmente os dois elementos do cluster devem ser instalados no site central, sendo que a critério do TCU e oportunamente, será necessária a mudança do segundo elemento do cluster para o *datacenter* de contingência;

1.3.1. a mudança prevista neste item será feita sem a utilização dos Serviços Técnicos Especializados, objeto do item 12;

1.4. possui fonte de alimentação 220V;

1.5. cada um dos nós do *cluster* deve:

1.5.1. proteger 3 (três) segmentos de rede físicos utilizando uma porta de comunicação dedicada para cada um dos segmentos;

1.5.2. possuir porta independente para gerência;

1.5.3. possuir porta independente para sincronismo de *cluster*;

1.5.4. possuir *throughput* de *firewall* de 3 (três) *Gbps*;

1.5.5. tratar 800.000 (oitocentas mil) sessões simultâneas;

1.5.6. admitir 30.000 (trinta mil) novas conexões por segundo;

1.5.7. suportar o tráfego gerado por todos os computadores da Rede TCU (aproximadamente 5.000 *hosts*);

1.6. implementa tecnologia de filtragem de pacotes baseada em estados (s*tateful inspection*);

1.7. registra os 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 sequencia de pacotes *TCP* e *status* dos *flags ACK*, *SYN* e *FIN*;

1.8. suporta toda a pilha de protocolos do modelo *TCP/IP*, com as seguintes funcionalidades:

1.8.1. faz inspeção *stateful* de tráfego;

1.8.2. suporta roteamento estático de tráfego;

1.8.3. randomiza o número de sequencia *TCP*, atuando como um *proxy* de número de sequencia *TCP*;

1.9. permite o funcionamento em modo transparente tipo *bridge* e permite ser configurado em alta disponibilidade neste modo;

1.10. integra-se com servidores de autenticação *RADIUS* ou *Microsoft Active Directory* (*LDAP* ou *Kerberos*), para administração;

1.11. permite a criação de regras por endereço de origem e destino, sub-rede IP, tipo de protocolo, porta de destino, interface de origem e tipo de serviço;

1.12. permite a definição de período de validade de regras, ou seja, determinar a validade de um horário e data;

1.13. implementa *NAT* (*Network Address Translation*) e *PAT* (*Protocol Address Translation*);

1.14. suporta *tags* de *VLAN trunking* (802.1q), sendo possível configurar 48 (quarenta e oito) *vlan-id* em uma mesma interface física;

1.15. suporta 1024 (um mil e vinte e quatro) regras de *firewall;*

1.16. permite a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

1.17. implementa sincronização do relógio utilizando o protocolo *NTP* para sincronizar com bases externas;

1.18. efetua proteção contra ataques de:

1.18.1. *SYN Flood*;

1.18.2. *IP Spoofing* e

1.18.3. *UDP Flood.*

1.19. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7 e *Windows XP*, atendendo aos seguintes requisitos:

1.19.1. permite a replicação de configurações e a aplicação de atualização de *software* para os elementos dos nós do *cluster*;

1.19.2. permite a definição de diferentes níveis de administração, sendo um nível completo e outro somente de visualização de configurações e *logs*;

1.19.3. permite a geração das seguintes informações, por período:

1.19.3.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

1.19.3.2. informações estatísticas de quantidade de conexões completadas e bloqueadas;

1.19.3.3. informações estatísticas de fluxo de tráfego e

1.19.3.4. informações estatísticas de quantidade de sessões ou conexões.

2. Serviços de *Firewall* e *VPN* Central Interno:

Quantidade: 1

Meses de Prestação: 60 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de *Firewall* e *VPN* Central Interno** deverão ser instalados no *datacenter* principal e no *datacenter* de contingência do TCU, ambos em Brasília. Deverão proteger os segmentos das redes interna e *DMZ* corporativas, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

2.1. providos com emprego de 2 (dois) elementos com função de *firewall* para serem fixados em *rack* padrão 19”*;*

2.2. implementa alta disponibilidade com tolerância a falhas, sendo admitida apenas a configuração ativo-ativo;

2.3. inicialmente os dois elementos do cluster devem ser instalados no site central, sendo que a critério do TCU e oportunamente, será necessária a mudança do segundo elemento do cluster para o datacenter de contingência;

2.3.1. a mudança prevista neste item será feita sem a utilização dos Serviços Técnicos Especializados, objetos do item 12;

2.4. possui fonte de alimentação 220V;

2.5. cada um dos nós do *cluster* deve:

2.5.1. proteger 8 (oito) segmentos de rede físicos utilizando uma porta de comunicação para cada um dos segmentos;

2.5.2. possuir porta para gerência independente;

2.5.3. possuir porta para sincronismo de *cluster* independente;

2.5.4. possuir *throughput* de *firewall* de 7 (sete) *Gbps*;

2.5.5. tratar 1.000.000 (hum milhão) de sessões simultâneas;

2.5.6. admitir 70.000 (setenta mil) novas conexões por segundo;

2.5.7. suportar o tráfego gerado por todos os computadores da Rede TCU (aproximadamente 5.000 *hosts*);

2.5.8. suportar 1024 (um mil e vinte e quatro) regras de *firewall*;

2.5.9. estabelecer túneis *IPSec* com *VPN throughput* de 60 (sessenta) *Mbps* para criptografia *3DES*.

2.6. implementa tecnologia de filtragem de pacotes baseada em estados (*Stateful Inspection*);

2.7. registra os 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 sequencia dos pacotes *TCP* e *status* dos *flags ACK*, *SYN* e *FIN*;

2.8. permite o funcionamento em modo transparente tipo *bridge* e permite ser configurado em alta disponibilidade neste modo;

2.9. integra-se com servidores de autenticação *RADIUS* ou *Microsoft Active Directory* (*LDAP* ou *Kerberos*), para administração;

2.10. permite a criação de regras por endereço de origem e destino, tipo de protocolo, porta de destino, interface de origem e tipo de serviço;

2.11. implementa *NAT* (*Network Address Translation*) e PAT (*Protocol Address Translation*);

2.12. implementa tratamento de QoS (Qualidade de Serviço) utilizando *DiffServ*;

2.13. suporta *tags* de *VLAN trunking* (802.1q), sendo possível configurar 48 (quarenta e oito) *vlan-id* em uma mesma interface física;

2.14. implementa sincronização do relógio utilizando o protocolo NTP para sincronizar com bases externas;

2.15. efetua proteção contra ataques:

2.15.1. *SYN Flood*;

2.15.2. *IP Spoofing;*

2.15.3. *UDP Flood;*

2.15.4. *Relay VPN.*

2.16. suporta os protocolos de roteamento *OSPF* e *PIM SM*;

2.17. possui funcionalidade de *DHCP Relay*;

2.18. estabelece túneis (*VPN site-to-site*) com todos os módulos de *VPN* remotos (29 sites);

2.18.1. implementa o protocolo *IPSec* e *IPSec NAT traversal*;

2.18.2. efetua trocas de chaves por meio do protocolo *IKE* e certificados X.509;

2.18.3. criptografa utilizando a especificação *AES (256 bits)*;

2.18.4. cada elemento do *cluster* admite 32 (trinta e dois) túneis concorrentes;

2.18.5. os túneis devem ser estabelecidos permanente de forma a evitar atrasos no encaminhamento de pacotes em caso de indisponibilidade da rede *MPLS*;

2.18.6. o tráfego somente deve ser encaminhado para o túnel quando a conexão *MPLS* estiver indisponível;

2.19. permite a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

2.20. permite criar dinamicamente, a partir da análise da sinalização *H.225* (*Call Setup*) e *H.245* (*Call Control*), as permissões pertinentes para o tráfego de mídia (*RTP*/*RTCP*) entre a *MCU* e as estações de videoconferência do TCU, consistindo essas permissões em combinações de:

2.20.1. *IP* e porta de origem (elemento originador da chamada);

2.20.2. *IP* e porta de destino (elemento chamado);

2.20.3. *Protocol-Type* do cabeçalho *IP* (*TCP*/*UDP*) e

2.20.4. interfaces de entrada e saída do tráfego de vídeo com inspeção *stateful*.

2.21. suporta as versões 1, 2, 3, 4 e 5 do *Framework H.323*;

2.21.1. será admitida a utilização de elemento externo ao *firewall* para suporte ao *Framework H.323,* desde que este elemento implemente, também, a funcionalidade de "travessia segura de *firewall*";

2.22. suporta *multicast*;

2.23. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7 e *Windows XP*, atendendo aos seguintes requisitos:

2.23.1. permite a replicação de configurações e a aplicação de atualização de *software* para os elementos dos nós do *cluster*;

2.23.2. permite a definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

2.23.3. permite a geração das seguintes informações, por período:

2.23.3.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

2.23.3.2. informações estatísticas de quantidade de conexões completadas e bloqueadas;

2.23.3.3. informações estatísticas de fluxo de tráfego e

2.23.3.4. informações estatísticas de quantidade de sessões ou conexões;

2.23.4. permite a visualização detalhada das conexões *VPN* estabelecidas, com volume de trafego e hora de início e fim, por conexão.

3. Serviços de *Firewall* e *VPN* Remoto:

Quantidade: 29

Meses de Prestação: 56 meses

Os equipamentos, produtos, peças ou *software*s necessários à prestação dos **Serviços de *Firewall* e *VPN* Remoto** deverão ser instalados nas Secretarias de Controle Externo do TCU nos Estados e no Instituto Serzedello Corrêa, conforme tabela de endereços presente no tópico XIII – Local de Execução dos Serviços – deste Termo, e deverão proteger segmentos distribuídos nas redes interna e *DMZ* de cada localidade, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

3.1. providos com emprego de 1 (um) elemento com função de *firewall* para ser fixado em *rack* padrão 19”*;*

3.2. possui fonte *bi-volt* com comutação automática;

3.3. protege 3 (três) segmentos de rede físicos utilizando 1 (uma) porta de comunicação para cada um dos segmentos;

3.4. possui porta independente para gerência;

3.5. possui *throughput* de *firewall* de 25 (vinte e cinco) *Mbps* (megabits por segundo);

3.6. trata 25.000 (vinte e cinco mil) sessões simultâneas;

3.7. admite 4.000 (quatro mil) novas conexões por segundo;

3.8. suporta o tráfego gerado por todos os computadores das redes protegidas (aproximadamente 200 *hosts*);

3.9. implementa tecnologia de filtragem de pacotes baseada em estados (Stateful Inspection);

3.10. registra os 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 sequencia dos pacotes TCP e status dos flags ACK, SYN e FIN;

3.11. permite o funcionamento em modo transparente tipo *bridge*;

3.12. integra-se com servidores de autenticação *RADIUS* ou *Microsoft Active Directory* (*LDAP* ou *Kerberos*), para administração;

3.13. permite a criação de regras por endereço de origem e destino, tipo de protocolo, porta de destino, interface de origem e tipo de serviço;

3.14. implementa *NAT* (*Network Address Translation*) e *PAT* (*Protocol Address Translation*);

3.15. implementa tratamento de *QoS* (Qualidade de Serviço) utilizando *DiffServ*;

3.16. suporta *tags* de *VLAN trunking* (802.1q), sendo possível configurar 20 (vinte) *vlan-id* em uma mesma interface física;

3.17. suporta 1024 (um mil e vinte e quatro) regras de *firewall;*

3.18. sincroniza relógio com bases externas utilizando o protocolo *NTP*;

3.19. efetua proteção contra ataques:

3.19.1. *SYN Flood*;

3.19.2. *IP Spoofing;*

3.19.3. *UDP Flood;*

3.19.4. *Relay VPN*.

3.20. possui funcionalidade de *DHCP Relay*;

3.21. estabelece túneis *IPSec* com *VPN throughput* de 8 (oito) *Mbps* para criptografia *3DES*;

3.22. estabelece túneis (*VPN site-to-site*) com o *site* central e com os *sites* remotos;

3.22.1. implementa o protocolo *IPSec* e *IPSec NAT traversal*;

3.22.2. efetua trocas de chaves por meio do protocolo *IKE* e certificados *X.509*;

3.22.3. criptografa utilizando a especificação *AES (256 bits)*;

3.22.4. admite 4 (quatro) túneis concorrentes;

3.22.5. os túneis devem ser estabelecidos permanentemente de forma a evitar atrasos no encaminhamento de pacotes em caso de indisponibilidade da rede *MPLS*;

3.22.6. o tráfego somente deve ser encaminhado para o túnel quando a conexão *MPLS* estiver indisponível;

3.23. permite a abertura de novas portas por fluxo de dados para serviços que requerem portas dinâmicas;

3.24. permite criar dinamicamente, a partir da análise da sinalização *H.225* (*Call Setup*) e *H.245* (*Call Control*), as permissões pertinentes para o tráfego de mídia (*RTP*/*RTCP*) entre a *MCU* e as estações de videoconferência do TCU, consistindo essas permissões em combinações de:

3.24.1. *IP* e porta de origem (elemento originador da chamada);

3.24.2. *IP* e porta de destino (elemento chamado);

3.24.3. *Protocol-Type* do cabeçalho *IP* (*TCP*/*UDP*) e

3.24.4. interfaces de entrada e saída do tráfego de vídeo com inspeção *stateful*.

3.25. configura *timeouts* distintos para a conexão de sinalização *H.323* e para as conexões de mídia dinamicamente negociadas (*RTP/RTCP*);

3.26. analisa os pacotes de manutenção do canal de controle *keepalives* de modo a garantir que a conexão de sinalização não necessite ser restabelecida a cada chamada;

3.27. suporta as versões 1, 2, 3, 4 e 5 do *Framework H.323*;

3.28. suporta *multicast*;

3.29. é administrado por ferramenta com interface gráfica única, remota e segura para as 29 (vinte e nove) localidades, a partir de plataforma *Windows* 7 e *Windows XP*, atendendo aos seguintes requisitos:

3.29.1. permite a replicação de configurações e a aplicação de atualização de *softwares* para todos os elementos desse serviço;

3.29.2. permite administração e *deploy* de políticas;

3.29.3. permite visualização de eventos (*logs*);

3.29.4. visualiza os dispositivos (*status up* ou *down*);

3.29.5. administra configurações de *VPN;*

3.29.6. permite a definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

3.29.7. permite a geração das seguintes informações, por período e elemento:

3.29.7.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

3.29.7.2. informações estatísticas de quantidade de conexões completadas e bloqueadas;

3.29.7.3. informações estatísticas de fluxo de tráfego e

3.29.7.4. informações estatísticas de quantidade de sessões ou conexões;

3.29.8. permite a visualização detalhada das conexões *VPN* estabelecidas, com volume de trafego e hora de início e fim por conexão.

4. Serviços de Prevenção de Intrusão Central:

Quantidade: 2

Meses de Prestação: 53 meses

Os equipamentos, produtos, peças ou *software*s necessários à prestação dos **Serviços de Prevenção de Intrusão Central** deverão ser instalados no *datacenter* principal e no *datacenter* de contingência do TCU, ambos em Brasília e deverão proteger segmentos distribuídos nas redes externa, interna e *DMZ*, com ligação física *in-line* e operação em modo *fail-open*, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

4.1. providos com emprego de 1 (um) ou mais elementos com função de *IPS* para serem fixados em *rack* padrão 19”, sendo que o conjunto dos requisitos especificados poderão ser atendidos por meio de uma das seguintes condições:

4.1.1. será admitida a utilização de produtos que sejam um módulo (desde que em *hardware* dedicado, ou seja, contendo requisitos de dimensionamento independentes) inserido no mesmo equipamento utilizado para atender ao item 2 – Serviços de *Firewall* e *VPN* Central Interno. Nesse caso, devem ser considerados os seguintes requisitos:

4.1.1.1. possui 8 (oito) interfaces físicas de rede, além das providas pelo item 2, podendo ser configuradas no modo *IDS*, monitorando 4 (quatro) segmentos ou no modo *IPS inline*, protegendo 4 (quatro) segmentos;

4.1.1.1.1. O licitante poderá fornecer as 8 (oito) interfaces adicionais em elemento externo ao alocado no item 2;

4.1.1.2. deverá ser configurada comunicação entre as interfaces físicas utilizadas nos Serviços de *Firewall* e *VPN* Central Interno e o item Serviços de Prevenção de Intrusão Central por meio do *backplane*, isto é, de modo a prover os serviços de *IPS* para as interfaces utilizadas no *firewall,* sem consumir interfaces físicas adicionais;

4.1.1.3. possui porta para gerência independente da porta provida para atender aos requisitos do Serviço de *Firewall* e *VPN* Central Interno;

4.1.2. caso sejam utilizados produtos diferentes daqueles relativos ao item 2 – Serviços de *Firewall* e *VPN* Central Interno, deverão ser considerados os seguintes requisitos:

4.1.2.1. possui 16 (dezesseis) interfaces físicas de rede, podendo ser configuradas no modo *IDS*, monitorando 8 (oito) segmentos ou no modo *IPS inline*, protegendo 8 (oito) segmentos;

4.1.2.2. possui porta independente para gerência.

4.2. possui fonte de alimentação 220V;

4.3. no caso de indisponibilidade do equipamento, possui mecanismo para não impedir o tráfego de pacotes para as redes escolhidas (*pass-through/fail-open*), sendo admitida a utilização de elemento externo para tal funcionalidade, desde que o dispositivo também seja *pass-through/fail-open*;

4.3.1. para o caso previsto no item 4.1.1, essa funcionalidade é requerida apenas para as 8 (oito) interfaces físicas adicionais;

4.4. possui *throughput* de inspeção de tráfego de 300 (trezentos) *Mbps* por interface;

4.4.1. caso seja utilizado 1 (hum) equipamento com 16 interfaces, o *throughput* deve ser de 4,8 (quatro inteiros e oito décimos) *Gbps*;

4.4.2. caso sejam utilizados 2 (dois) ou mais equipamentos, o *throughput* de cada um deve ser de 2,4 (dois inteiros e quatro décimos) *Gbps*;

4.4.3. para o caso previsto no item 4.1.1 o *throughput* de inspeção de tráfego deverá ser de:

4.4.3.1. 2,4 (dois inteiros e quatro décimos) *Gbps* para as interfaces compartilhadas com o item 2;

4.4.3.2. para as 8 (oito) interfaces adicionais deve possuir *throughput* de inspeção de tráfego de 300 (trezentos) *Mbps* por interface, seguindo a mesma lógica descrita nos itens 4.4.1 a 4.4.2;

4.5. trata 80.000 (oitenta mil) sessões simultâneas por interface;

4.5.1. caso seja utilizado 1 (hum) equipamento com 16 interfaces, deve tratar 1.280.000 (hum milhão, duzentos e oitenta mil) sessões simultâneas;

4.5.2. caso sejam utilizados 2 (dois) ou mais equipamentos, cada um deles deve tratar 640.000 (seiscentos e quarenta mil) sessões simultâneas;

4.5.3. para o caso previsto no item 4.1.1, o equipamento deverá tratar:

4.5.3.1. 640.000 (seiscentas e quarenta mil) sessões simultâneas para as interfaces compartilhadas com o item 2;

4.5.3.2. para as 8 (oito) interfaces adicionais, deve tratar 80.000 (oitenta mil) sessões simultâneas por interface, seguindo a mesma lógica descrita nos itens 4.5.1 a 4.5.2;

4.6. suporta o tráfego gerado por todos os computadores da Rede TCU (aproximadamente 5.000 *hosts*);

4.7. inicialmente os dois elementos devem ser instalados no site central, sendo que, a critério do TCU e oportunamente, será necessária a mudança do segundo para o *datacenter* de contingência;

4.8. funciona em modo *IDS* (passivo/monitoração/*learning*) e *IPS* (ativo/proteção), simultaneamente, em portas distintas;

4.9. funciona em modo de teste, de forma a coletar informações de tráfego para formação de *baseline* e posterior definição e aplicação de regras;

4.10. faz inspeção profunda de pacotes (*DPI*), incluindo o *payload*, identificando perfis de tráfego anômalos, inclusive na modalidade *Stateful Inspection;*

4.11. detecta e previne ataques não orientados a conexão (*stateless*);

4.12. suporta toda a pilha de protocolos do modelo *TCP*/*IP*;

4.13. faz inspeção *stateful* de tráfego;

4.14. permite a aplicação de novas políticas sem interrupção de trafego;

4.15. cria regras dinâmicas de assinaturas para protocolos não padronizados;

4.16. detecta e interrompe o tráfego de rede que tenha como finalidade ou efeito colateral causar danos à informação, indisponibilidade de sistemas ou ainda o consumo não autorizado de recursos da rede TCU;

4.17. executa as suas funções sem a instalação de agentes nos *hosts* a serem protegidos;

4.18. identifica *hosts* conectados à rede que apresentem comportamento anormal potencialmente danoso, como propagação de *malwares* e *botnets*;

4.19. deve possuir compatibilidade aos serviços do item 9 – Serviços de Gestão de Vulnerabilidades – de maneira a diminuir falsos positivos e aprimorar a detecção de ameaças que não possuam assinaturas mapeadas;

4.20. captura e armazena o perfil comportamental de cada dispositivo de rede, disponibilizando relatórios com as seguintes informações:

4.20.1. endereço *IP*;

4.20.2. sistema operacional;

4.20.3. serviços e portas utilizadas;

4.20.4. tipo e volume de trafego;

4.20.5. aplicativos;

4.20.6. vulnerabilidades associadas a cada perfil de dispositivo;

4.21. identifica serviços sendo executados em portas não autorizadas;

4.22. identifica ataques que utilizam tráfego interativo;

4.23. identifica ataques com múltiplos fluxos;

4.24. executa bloqueio automático do tráfego oriundo e destinado a *hosts* cujo comportamento esteja fora de conformidade com as políticas estabelecidas, ou seja, identificado como efetivamente ou potencialmente danoso, como, por exemplo, bloqueia automaticamente *host* de origem para qual tenha sido disparada uma assinatura de ataque e termina automaticamente conexão *TCP* para a qual tenha sido disparada uma assinatura de ataque;

4.25. suporta assinaturas, seja nativamente ou por meio de configurações, para protocolos de aplicação, entre os quais devem constar, no mínimo, os seguintes:

4.25.1. *HTTP, SMTP, FTP, RPC (MS-RPC), POP3, TELNET, DNS, IMAP, DHCP, TFTP, NNTP, RTSP, SNMP, SNMP trap v1, SYSLOG, SSH, SMB (NetBIOS), MS-RPC, VNC, NTP, LDAP, NBNAME, SSL, NBDS* e *RADIUS;*

4.25.2. *AOL-IM, Yahoo-IM e Microsoft Live Messenger;*

4.25.3. *eMule, eDonkey, Kazaa, Napster* e *WinMX;*

4.25.4. *H.225, MGCP* e *SIP.*

4.26. protege e analisa ataques desconhecidos sem atualização de assinaturas, por meio de acesso a informações no site do fabricante (*cloud computing*);

4.27. efetua análise comportamental baseada no acesso ao site do fabricante (*cloud computing*) para identificar códigos maliciosos originados em servidores e direcionados aos clientes;

4.28. mantém dados sobre ataques, com o número de vezes que um ataque ocorreu, quando e de que forma ele ocorreu e informações sobre quais aplicações foram usadas.

4.29. reconhece e responde a ataques à rede e aos *hosts*, em tempo real;

4.30. efetua proteção contra ataques:

4.30.1. *DDoS* (*distributed denial of service*) e *DOS* (*Denial of Service*);

4.30.2. *SYN Flood*;

4.30.3. *UDP Flood*.

4.30.4. *Spywares*;

4.30.5. estouro de pilha *(buffer overflow);*

4.30.6. dia-zero *(zero-day);*

4.30.7. tráfego mal formado;

4.30.8. cabeçalhos inválidos de protocolo;

4.30.9. múltiplos pacotes (fragmentação).

4.31. permite configurar recursos de:

4.31.1. *TCP connection limiting*;

4.31.2. limite de requisições por protocolo (*UDP*, *TCP*);

4.32. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7 e *Windows XP*, atendendo aos seguintes requisitos:

4.32.1. permite a replicação de configurações e a aplicação de atualização de *softwares* entre os elementos desse Serviço;

4.32.2. permite a definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

4.32.3. permite a geração das seguintes informações, por período e elemento:

4.32.3.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

4.32.3.2. informações estatísticas de quantidade de conexões completadas e bloqueadas;

4.32.3.3. informações estatísticas de fluxo de tráfego;

4.32.3.4. informações estatísticas de quantidade de sessões ou conexões e

4.32.3.5. informações estatísticas de quantitativo de ataques identificados por tipo.

5. Serviços de *Proxy/cache* com filtro de conteúdo *WEB*:

Quantidade: 1

Meses de Prestação: 57 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de *Proxy/cache* com filtro de conteúdo *WEB*** deverão ser instalados no *datacenter* principal e no *datacenter* de contingência do TCU, ambos em Brasília, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

5.1. providos com emprego de 2 (dois) elementos com função de *Proxy/Cache* com filtro de conteúdo *WEB*, para serem fixados em *rack* padrão 19”*;*

5.2. implementa alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo;

5.3. inicialmente os dois elementos do *cluster* devem ser instalados no site central, sendo que a critério do TCU e oportunamente, será necessária a mudança do segundo elemento do *cluster* para o *datacenter* de contingência;

5.3.1. a mudança prevista neste item será feita sem a utilização dos Serviços Técnicos Especializados, objetos do item 12;

5.4. possui fonte de alimentação 220V;

5.5. cada um dos nós do *cluster* deve:

5.5.1. suportar o tráfego de acesso à internet oriundo da rede interna com 5.000 (cinco mil) hosts (usuários simultâneos) e *throughput* de 100 (cem) *Mbps*;

5.5.2. analisar tráfego de, pelo menos, 850 (oitocentos e cinquenta) *requests HTTPS*/segundo;

5.5.3. armazenar as informações do cache utilizando tecnologia que possua capacidade útil de *500MB*, permita a substituição de unidade de disco defeituosa sem a necessidade de parada do serviço e utilize discos de alta velocidade (*SAS* ou *SCSI Ultra*);

5.6. faz *proxy* para *HTTP* (*Hypertext Transfer Protocol*), *HTTPS* (*Hypertext Transfer Protocol Secure*), *DNS*, *FTP* (*File Transfer Protocol*) e *FTP* transportado em túnel *HTTP*;

5.7. faz cache para *HTTP* (*Hypertext Transfer Protocol*), *DNS*, *FTP* (*File Transfer Protocol*) e *FTP* transportado em túnel *HTTP*;

5.8. opera os modos *proxy* explícito e *proxy* transparente, podendo ser configurado para operar em um dos dois modos de operação;

5.9. filtra o trafego criptografado via *SSL* (porta 443), tanto na entrada quanto na saída (*inbound* e *outbound*), atuando como *man-in-the-middle;*

5.10. verifica certificados de *URL* solicitadas, permitindo bloqueio, caso o certificado seja classificado como inválido; e

5.11. aplica para o conteúdo criptografado os mesmos filtros utilizados para os protocolos *HTTP* e *FTP*.

5.12. implementa o protocolo *WCCP* versão 2;

5.13. implementa cache de consultas *DNS*;

5.14. implementa cache de objetos, inclusive de arquivos com extensão *PDF*;

5.15. é transparente para tráfego não-*HTTP*, de modo que pacotes que utilizem as portas padrão do protocolo *HTTP*, com conteúdo diverso, não sofram interferência em função da presença do *proxy*/cache na rede;

5.16. implementa filtros de *URL* bidirecionais (*inbound* e *outbound*) incluindo o exame de conteúdo de todas as requisições e respostas (*requests* e *responses*);

5.17. implementa filtros de *URL* customizados por políticas;

5.18. implementa filtros de *URL* baseados em base de dados armazenada localmente nos equipamentos;

5.19. bloqueia requisições por meio de filtros de extensão de arquivos;

5.20. implementa controle de acesso a sites *HTTP*, *HTTPS* e *FTP* baseado em lista negra e lista branca;

5.21. controla o acesso a sites *HTTP*, *HTTPS* e *FTP*, permitindo a definição de perfis de acesso diferenciados para determinados serviços, endereços de origem, endereços de destinos, domínios, *URLs*, faixa de tempo, e usuários e grupos da rede Windows (utilizando a base de usuários e grupos do *Active Directory*);

5.22. permite ou bloqueia sites ou categorias de sites, por:

5.22.1. usuário do *Active Directory*;

5.22.2. grupo do *Active Directory* e

5.22.3. faixa de tempo.

5.23. permite o uso de *wildcards*, máscaras ou expressões regulares, permitindo que seja filtrado conteúdo presente no *header HTTP*;

5.24. a base de *URLs* deve ser atualizada automaticamente, por meio de conexão internet, no site do fabricante e deve possuir:

5.24.1. 20 (vinte) milhões de sites (domínios) registrados em 70 (setenta) categorias pré-definidas;

5.24.2. sites em 5 (cinco) idiomas, incluindo, necessariamente, inglês, português e espanhol;

5.25. permite a criação de categorias customizadas (*user defined*);

5.26. permite que qualquer site seja colocado manualmente em categoria customizada, diferente da original categorização de reputação do site.

5.27. define tempo de expiração de conexões para os protocolos *HTTP*, *HTTPS*, *FTP*;

5.28. bloqueia "*scripts*" como *Active X, Java, Javascript* e *VBScript*;

5.29. bloqueia *download* de arquivos por meio das seguintes formas:

5.29.1. leitura dos *bytes* iniciais do arquivo (*file header signature*);

5.29.2. parâmetro tipo de conteúdo (*Content-Type*) no cabeçalho da resposta *HTTP* e

5.29.3. extensão do arquivo a ser recebido.

5.30. controla aplicações *WEB*, sendo possível definir ações de monitoramento e bloqueio de aplicações, incluindo:

5.30.1. *Instant Messaging;*

5.30.2. *Webmail Attachments;*

5.30.3. *Streaming Media.*

5.31. filtra conteúdo por meio de filtros de *pop-ups*;

5.32. registra regras de exceção a sites *HTTPS* que não devem ter seu tráfego inspecionado;

5.33. bloqueia clientes por versão de *software* ou tipo de *browser*;

5.34. detecta e bloqueia *user agent* suspeitos;

5.35. define políticas que possam ser aplicadas por:

5.35.1. categorias;

5.35.2. reputação do site;

5.35.3. horários do dia;

5.35.4. dias da semana;

5.35.5. endereço *IP*;

5.35.6. usuário do *Active Directory*;

5.35.7. grupo do *Active Directory*;

5.35.8. expressões de *request* de *URL* e

5.35.9. terminação de *URLs* (ex. “gov.br”).

5.36. integra-se com solução de antivírus de *gateway* por meio do protocolo *ICAP* ou possui a solução de antivírus incorporada no produto;

5.37. inspeciona conteúdo para verificação e eliminação de vírus e *malwares*;

5.38. limita o tempo máximo permitido para *scan* de arquivos;

5.39. permite 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);

5.40. efetua análise de objetos encapsulados com a opção de bloqueio;

5.41. as verificações de *malware* devem ocorrer de forma concorrente para cada objeto analisado, em tempo real, sem enfileiramento;

5.42. armazena o resultado das verificações de *malware* em cache;

5.43. verifica tráfego analisando os dados até a camada 4 do modelo *OSI*, identificando estações de trabalho da rede interna possivelmente infectadas por *malwares*.

5.44. identifica e bloqueia aplicações maliciosas, inclusive dos tipos:

5.44.1. *Java Scripts;*

5.44.2. *Java applets;*

5.44.3. *Java applications;*

5.44.4. *ActiveX;*

5.44.5. *Flash ActionScripts;*

5.44.6. executáveis *Windows;*

5.44.7. *Visual Basic;*

5.44.8. potencialmente não desejados *(spywares);*

5.45. bloqueia todos os comportamentos/técnicas abaixo:

5.45.1. *phishing (para webmail);*

5.45.2. *data theft: Backdoor;*

5.45.3. *data theft: Keylogger;*

5.45.4. *data theft: Password stealer;*

5.45.5. *system compromise: Code execution exploit;*

5.45.6. *system compromise: Browser exploit;*

5.45.7. *system compromise: Trojan;*

5.45.8. *stealth activity: Rootkit;*

5.45.9. *viral Replication: Network worm;*

5.45.10. *viral Replication: File infector vírus;*

5.45.11. *system compromise: Trojan downloader;*

5.45.12. *system compromise: Trojan dropper;*

5.45.13. *system compromise: Trojan proxy;*

5.45.14. *web threats: Infected website;*

5.45.15. *stealth activity: Code injection;*

5.45.16. *detection evasion: Obfuscated code;*

5.45.17. *detection evasion: Packed code;*

5.45.18. *potentially unwanted: Ad-/Spyware;*

5.45.19. *potentially unwanted: Adware;*

5.45.20. *data theft: Spyware;*

5.45.21. *potentially unwanted: Dialer;*

5.45.22. *web threats: Vulnerable ActiveX controls;*

5.45.23. *potentially unwanted: Suspicious activity;*

5.45.24. *web threats: Cross-site scripting;*

5.45.25. *potentially unwanted: Deceptive behavior;*

5.45.26. *potentially unwanted: Redirector;*

5.45.27. *potentially unwanted: Direct kernel communication;*

5.45.28. *potentially unwanted: Privacy violation.*

5.46. possui mecanismo que permite ao administrador do sistema definir determinada página como resposta quando a *URL* for bloqueada;

5.47. possui mecanismo que permite emitir os seguintes relatórios, nos formatos *HTML*, *PDF* e *CSV*:

5.47.1. sites com maior volume de dados acessados por usuário;

5.47.2. sites acessados por determinados usuários (ou *IPs*), classificado por *username*, *IP* ou data/hora;

5.47.3. sites bloqueados por determinados usuários (ou *IPs*), classificado por *username*, *IP* ou data/hora;

5.47.4. usuários que acessaram determinado site por determinado período;

5.47.5. *sites* bloqueados (*top100*);

5.47.6. vírus encontrados (*top100*);

5.47.7. computadores e usuários (*top100*) que mais acessaram páginas *HTTP* e *HTTPS*, em *MB*;

5.47.8. computadores e usuários (*top100*) que tiveram mais requisições bloqueadas;

5.47.9. estatísticas de acesso *HTTP* e *HTTPS* por site (*top100*) em volume de dados (*MB*);

5.47.10. estatísticas de acesso *HTTP* e *HTTPS* por sub-rede *IP* em volume de dados (*MB*);

5.47.11. estatísticas de acesso *HTTP* e *HTTPS* por sub-rede *IP* e por computadores e usuários, em volume de dados (*MB*);

5.47.12. estatísticas de acesso *HTTP* e *HTTPS* por extensão de arquivo acessado em volume de dados (*MB*).

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

5.49. integra-se com servidores de autenticação *Microsoft Active Directory* (*LDAP* ou *Kerberos*) para implementação de regras baseadas em usuários/grupos do serviço de diretórios;

5.50. integra-se com servidores de autenticação *RADIUS* ou *Microsoft Active Directory* (*LDAP* ou *Kerberos*), para administração;

5.51. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7 e *Windows XP*, atendendo aos seguintes requisitos:

5.51.1. permite a replicação de configurações e a aplicação de atualização de *softwares* para todos os elementos que compõe este serviço;

5.51.2. permite a definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

5.51.3. permite a geração das seguintes informações, por período e elemento:

5.51.3.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

5.51.3.2. informações estatísticas de quantidade de conexões completadas e bloqueadas;

5.51.3.3. informações estatísticas de fluxo de tráfego;

5.51.3.4. informações estatísticas de quantidade de sessões ou conexões e

5.51.3.5. informações estatísticas de quantitativo de ataques identificados por tipo.

6. Serviços de *SMTP Antispam*:

Quantidade: 1

Meses de Prestação: 57 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de *SMTP Antispam*** deverão ser instalados no *datacenter* principal e no *datacenter* de contingência do TCU, ambos em Brasília, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

6.1. providos com emprego de 2 (dois elementos com função de *relay SMTP* e *antispam*, para serem fixados em *rack* padrão 19”*;*

6.2. implementa alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo;

6.3. inicialmente os dois elementos do cluster devem ser instalados no site central, sendo que a critério do TCU e oportunamente, será necessária a mudança do segundo elemento do cluster para o datacenter de contingência;

6.3.1. a mudança prevista neste item será feita sem a utilização dos Serviços Técnicos Especializados, objetos do item 12;

6.4. possui fonte de alimentação 220V;

6.5. será admitida a configuração da alta disponibilidade por meio de prioridades em registros do tipo *MX* no *DNS* do Tribunal;

6.6. implementa o protocolo *SMTP* (*Simple Mail Transfer Protocol*);

6.7. cada um dos nós do *cluster* deve:

6.7.1. proteger 5.000 (cinco mil) caixas postais de correio eletrônico, com taxa média de 12.000 mensagens encaminhadas para análise, por hora;

6.7.2. possuir *throughput* para gerenciar 5.000 (cinco mil) conexões *SMTP* simultâneas;

6.7.3. para que seja possível a liberação de emails de quarentena pelo usuário, a interface para tal fim deve permitir 500 (quinhentas) conexões simultâneas;

6.8. suporta os padrões *Sender Policy Framework* e *SenderID;*

6.9. suporta autenticação *TLS* (*Transport Layer Security*)

6.10. controla sessões *SMTP* e limita o trafego de mensagens baseado em endereço *IP*, range de *IPs*, *subnet IP*, nome de domínio, nome parcial de domínio e reputação do emissor;

6.11. inspeciona e bloqueia mensagens baseado em:

6.11.1. tamanho de mensagem;

6.11.2. número de destinatários por mensagem;

6.11.3. número de mensagens por conexão e

6.11.4. número de conexões simultâneas, por *IP*.

6.12. restringe conexões baseado no número máximo de destinatários por hora;

6.13. limita o número máximo de conexões simultâneas;

6.14. verifica *DNS* reverso;

6.15. rejeita mensagens para destinatários inválidos durante o dialogo *SMTP* (trata *Non-Delivery Report Attack*);

6.16. previne ataque de diretório *(Directory Harvest Attack*);

6.17. protege contra dia-zero (*zero-day*);

6.18. penaliza servidores atacantes (*Spam Throttling*) com opção de customização do mecanismo;

6.19. controla *bounce* de e-mail;

6.20. remove condicionalmente o corpo da mensagem e anexos específicos em um e-mail da *Internet* e também em ações *HTTP POST* e *Phishing Scam*;

6.21. implementa nas mensagens de saída categorização a partir de políticas preestabelecidas;

6.22. integra-se com solução de antivírus de *gateway* por meio do protocolo ICAP ou tem por padrão a solução de antivírus incorporada na solução;

6.23. possui listas negras e listas brancas para domínios e usuários;

6.24. detecta anexos criptografados, permitindo a definição da ação a ser executada;

6.25. detecta anexos compactados em múltiplos formatos, incluindo *zip* e *rar* (até dez camadas de compactação), definindo ação a ser executada;

6.26. identifica arquivos anexados pelo seu tipo real, pelo seu nome, pela sua extensão e pelo seu tipo *MIME*;

6.27. faz busca por palavras em anexos, sendo possível definir o número de ocorrências para considerar *SPAM*;

6.28. filtra conteúdo, permitindo a concatenação, por operações booleanas, de regras que verifiquem a ocorrência de expressões (expressões regulares) nos campos do cabeçalho *SMTP*, nos anexos e no corpo da mensagem

6.29. filtra conteúdo analisando:

6.29.1. assinaturas para corpo da mensagem e anexos;

6.29.2. heurística, por meio de análise de cabeçalhos, conteúdo e estrutura da mensagem;

6.29.3. filtro de reputação (*IP*/Domínio do remetente);

6.29.4. *URL's*;

6.29.5. filtros *anti-phishing*;

6.30. armazena mensagens classificadas como *SPAM* em quarentena;

6.31. faz a quarentena por usuário integrando-se com servidores de autenticação *Microsoft Active Directory* (*LDAP* ou *Kerberos*);

6.32. possibilita que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são *SPAM*;

6.33. o módulo de quarentena deverá ser capaz de enviar notificação periódica para os usuários, informando as mensagens consideradas como *SPAM* que foram inseridas na quarentena;

6.34. remove automaticamente as mensagens armazenadas em quarentena de acordo com as configurações definidas pelo administrador;

6.35. permite que o usuário cadastre endereços de email em listas negras/listas brancas pessoais;

6.36. permite armazenar 30 dias de mensagens em quarentena, podendo o limite ser ajustado para valor inferior, de acordo com as políticas vigentes durante a execução do contrato;

6.37. integra-se com servidores de autenticação *Microsoft Active Directory* (*LDAP* ou *Kerberos*) para verificação de destinatários validos;

6.38. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7 e *Windows XP*, atendendo aos seguintes requisitos:

6.38.1. permite replicação de configurações e aplicação de atualização de *softwares* para todos os elementos que compõe este serviço;

6.38.2. permite definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

6.38.3. permite geração das seguintes informações, por período e elemento:

6.38.3.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

6.38.3.2. informações estatísticas de quantidade de conexões completadas e bloqueadas;

6.38.3.3. informações estatísticas de fluxo de tráfego;

6.38.3.4. informações estatísticas de quantidade de sessões ou conexões e

6.38.3.5. informações estatísticas de quantitativo de ataques identificados por tipo.

7. Serviços de *Firewall* de Aplicação:

Quantidade: 1

Meses de Prestação: 53 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de *Firewall* de Aplicação** deverão ser instalados no *datacenter* principal e no *datacenter* de contingência do TCU, ambos em Brasília, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

7.1. providos com emprego de 2 (dois) elementos com função de *firewall* de aplicação (*WAF*) para serem fixados em *rack* padrão 19”*;*

7.2. implementa alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo;

7.3. inicialmente os dois elementos do cluster devem ser instalados no site central, sendo que a critério do TCU e oportunamente, será necessária a mudança do segundo elemento do cluster para o datacenter de contingência;

7.3.1. a mudança prevista neste item será feita sem a utilização dos Serviços Técnicos Especializados, objetos do item 12;

7.4. possui fonte de alimentação 220V;

7.5. cada um dos nós do *cluster* deve:

7.5.1. proteger 3 (três) segmentos de rede físicos utilizando duas portas de comunicação para cada um dos segmentos*;*

7.5.2. possuir porta independente para gerenciamento;

7.5.3. possuir porta independente para sincronismo de *cluster*;

7.5.4. inspecionar 1 (um) *Gbps* de tráfego de application *firewall*;

7.5.5. processar 800 (oitocentos) *Kpps* (milhares de pacotes por segundo);

7.5.6. admitir 35.000 (trinta e cinco mil) novas conexões por segundo (transações por segundo – *TPS*);

7.6. suporta agregação de portas (*trunk*);

7.7. suporta o protocolo 802.1q;

7.8. analisa tráfego *HTTP*/0.9, *HTTP*/1.0 e *HTTP*/1.1;

7.9. restringe métodos *HTTP*/*HTTPS* permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*;

7.10. permite as seguintes opções de implementação:

7.10.1. monitoramento (*sniffing*);

7.10.2. *proxy* (reverso e transparente).

7.11. permite que novas políticas fiquem apenas monitorando o tráfego, sem bloqueá-lo, indicando caso aconteça algum evento;

7.12. remove as mensagens de erro do conteúdo que será enviado aos usuários;

7.13. em modo "monitoramento" (*sniffing*), realiza análise e avaliação do tráfego, gera relatórios com os dados analisados e simula bloqueios para efeito de avaliação;

7.14. protege 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;

7.15. bloqueia ataques aos servidores de aplicação, por meio dos seguintes recursos:

7.15.1. identifica, isola e bloqueia ataques sofisticados sem impactar nas transações das aplicações;

7.15.2. identifica, isola e bloqueia ataques sofisticados para os protocolos: *HTTP* e *HTTPS*;

7.15.3. permite a utilização de modelo positivo de segurança para proteger contra ataques às aplicações *HTTP* e *HTTPS*, além de proteger contra ataques conhecidos aos protocolos *HTTP* e *HTTPS*;

7.15.4. quando detectada uma tentativa de ataque bloqueia de imediato o tráfego ou a sessão;

7.15.5. bloqueia com intermediação e interrupção da conexão;

7.15.6. cria políticas automáticas que bloqueiam o endereço *IP* que realizar violações;

7.15.7. utiliza página *HTML* informativa e personalizável como *HTTP Response* aos bloqueios;

7.15.8. configura políticas de bloqueio baseadas em requisição *HTTP*, endereço *IP* e usuário de aplicação.

7.16. apenas transações de aplicações validadas devem ser aceitas, 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;

7.17. identifica e armazena o ataque acontecido com detalhes, com as seguintes informações:

7.17.1. nome do ataque;

7.17.2. qual campo foi atacado;

7.17.3. quantas vezes esse ataque foi realizado;

7.17.4. cópia da tentativa do ataque;

7.17.5. horário do ataque e

7.17.6. endereços *IP* que originaram os ataques.

7.18. armazena informações de identificação dos usuários autenticados nas aplicações;

7.19. suporta *request compression* e *response compression*;

7.20. assina *cookies* digitalmente e edita endereços de *URL* ("*URL Rewriting*");

7.21. protege as aplicações de banco de dados contra ataques conhecidos, monitora e controla os acessos e atividades relacionadas às bases de dados;

7.22. suporta aplicações que utilizam autenticação com estes métodos:

7.22.1. autenticação básica;

7.22.2. *NTLM* e

7.22.3. certificados *SSL*.

7.23. para as soluções que utilizam *SSL* para transferência de dados, os certificados e pares de chaves pública/privada devem ser importados (atua como *man-in-the-middle* para tráfego *SSL*);

7.24. possui 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*;

7.25. identifica e cria perfil de utilização dos aplicativos, inclusive desenvolvidos em *Javascript*, *CGI*, *ASP* e *PHP*;

7.26. o perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

7.27. correlaciona múltiplos eventos de segurança em conjunto para distinguir de forma precisa o tráfego permitido do tráfego malicioso;

7.28. identifica ataques baseados em:

7.28.1. assinaturas, com atualização diária da base pelo fabricante;

7.28.2. regras e

7.28.3. perfis de utilização.

7.29. detecta ataques de força bruta por meio dos seguintes métodos:

7.29.1. aumento do tempo de resposta da aplicação monitorada;

7.29.2. quantidade de transações por segundo (*TPS*), monitorando a quantidade de transações por segundo por endereço IP;

7.30. detecta ataques do tipo força bruta em que:

7.30.1. o atacante solicita repetidamente o mesmo recurso;

7.30.2. o atacante realiza repetidas tentativas não autorizadas de acesso e

7.30.3. são utilizados ataques automatizados de *login*.

7.31. detecta ataques do tipo força bruta que explorem:

7.31.1. controles de acesso da aplicação (Erro 401 – *Unauthorized*);

7.31.2. solicitações repetidas ao mesmo recurso, em qualquer parte/*URL* da aplicação;

7.31.3. aplicações *WEB* que não retornam o erro 401 por meio da identificação de expressão regular no retorno/página de erro da aplicação);

7.31.4. gerenciamento de sessão (muitas sessões de um único endereço *IP* ou a um range de *IPs*) e

7.31.5. clientes automatizados (robôs, requisições muito rápidas).

7.32. configura política de segurança para as aplicações:

7.32.1. *Microsoft Outlook WEB Access;*

7.32.2. *Microsoft ActiveSync;*

7.32.3. *Oracle Applications (APPEX) e*

7.32.4. *Microsoft Office SharePoint.*

7.33. permite a criação de políticas diferenciadas por aplicação e por *URL*, onde cada aplicação e *URL* poderão ter políticas totalmente diferentes;

7.34. possui mecanismo para criação dinâmica de política de segurança, com aprendizado automático de padrão de utilização da aplicação, realizado sobre o fluxo de tráfego bi-direcional atravessando o equipamento;

7.35. filtra e valida funções *XML* específicas da aplicação;

7.36. possibilita atualização de novas assinaturas para ataques conhecidos;

7.37. apresenta proteção positiva e segura contra ataques, como:

7.37.1. *Anonymous Proxy Vulnerabilities;*

7.37.2. *Brute Force Login;*

7.37.3. *Buffer Overflow;*

7.37.4. *Cookie Injection;*

7.37.5. *Cookie Poisoning;*

7.37.6. *Cross Site Request Forgery (CSRF);*

7.37.7. *Cross Site Scripting (XSS);*

7.37.8. *Data Destruction;*

7.37.9. *Directory Traversal;*

7.37.10. *Forceful Browsing;*

7.37.11. *Form Field Tampering;*

7.37.12. *Google Hacking;*

7.37.13. *HTTP Denial of Service;*

7.37.14. *HTTP parameter pollution;*

7.37.15. *HTTP hidden field manipulation;*

7.37.16. *HTTP request smuggling;*

7.37.17. *HTTP Response Splitting;*

7.37.18. *HTTP Verb Tampering;*

7.37.19. *Illegal Encoding;*

7.37.20. *Known Worms;*

7.37.21. *LDAP injection;*

7.37.22. *Malicious Encoding;*

7.37.23. *Malicious Robots;*

7.37.24. *OS Command Injection;*

7.37.25. *Parameter Tampering;*

7.37.26. *Remote File Inclusion Attacks;*

7.37.27. *Sensitive Data Leakage (Social Security Numbers, Cardholder Data, PII, HPI);*

7.37.28. *Session Hijacking;*

7.37.29. *Site Reconnaissance;*

7.37.30. *SQL Injection;*

7.37.31. *Web Scraping;*

7.37.32. *Web server software and operating system attacks;*

7.37.33. *Web Services (XML) attacks;* e

7.37.34. *Zero Day Malware;*

7.38. permite configurar granularmente, por aplicação protegida, restrições de métodos *HTTP* permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de *cookies*;

7.39. permite definir regras de tamanho para *upload* de arquivos pelo método *PUT*, com as seguintes restrições:

7.39.1. tamanho por arquivo;

7.39.2. tamanho por conjunto de arquivos;

7.39.3. quantidade de arquivos;

7.40. a criação das políticas deve possuir as formas:

7.40.1. automático por meio da observação do tráfego para a aplicação;

7.40.2. automático por meio da observação do tráfego de teste e

7.40.3. manual.

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

7.41.1. tempo de resposta de uma página *web*;

7.41.2. tamanho da resposta de uma página *web*;

7.41.3. *user-agent* (navegador);

7.41.4. usuário;

7.41.5. horário;

7.41.6. *IP* de origem;

7.41.7. assinatura de ataque;

7.41.8. conteúdo do *payload*;

7.41.9. conteúdo do cabeçalho;

7.41.10. conteúdo da *cookie*;

7.41.11. código de *response*;

7.41.12. *hostname*;

7.41.13. tipo de protocolo (*HTTP* ou *HTTPS*);

7.41.14. parâmetro;

7.41.15. número de ocorrências em determinado intervalo de tempo;

7.41.16. método *HTTP*;

7.42. permite criação de assinaturas de ataques;

7.43. reconhece assinaturas seletivas, e filtros de ataque que devem proteger contra:

7.43.1. ataques de negação de serviços automatizados;

7.43.2. *worms* e vulnerabilidades conhecidas;

7.43.3. *requests* em objetos restritos.

7.44. previne contra vazamentos dos códigos dos servidores;

7.45. protege contra as 10 maiores vulnerabilidades da lista *OWASP*;

7.46. exporta requisições que contém os ataques, nos formatos *PDF* e *CSV*;

7.47. realiza localização geográfica do *IP*, identificando pais de origem da requisição;

7.48. aprende o comportamento da aplicação:

7.48.1. campos, valores, *cookies* e *URLs*;

7.48.2. políticas sugeridas somente devem ser aplicadas após um período configurável;

7.49. inspeciona e monitora até a camada de aplicação, todo tráfego de dados *HTTP*, incluindo cabeçalhos, campos de formulários e conteúdo, além de inspecionar os *requests* e *responses*;

7.50. as checagens devem ser realizadas 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*;

7.51. protege contra mensagens *XML* e *SOAP* malformadas;

7.52. utiliza o campo *HTTP X-Forwarded-For* sem modificar seu conteúdo de origem, permitindo a diferenciação em ambientes com *NAT*;

7.53. suporta *SSL offload*;

7.54. remove as mensagens de erro do conteúdo que será enviado aos usuários;

7.55. emite os seguintes relatórios:

7.55.1. gráfico indicando tipo de ataque;

7.55.2. gráfico indicando tipo de violação;

7.55.3. gráfico indicando quais *URLs* foram atacadas;

7.55.4. gráfico indicando severidade;

7.55.5. gráfico indicando os endereços *IPs* de origem e

7.55.6. gráfico indicando a localização geográfica dos endereços *IPs* de origem.

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

7.57. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7 e *Windows XP*, atendendo os seguintes requisitos:

7.57.1. permite a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

7.57.2. permite a replicação de configurações e a aplicação de atualização de *softwares* para os elementos dos nós do *cluster*;

7.57.3. permite a geração das seguintes informações, por período:

7.57.3.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

7.57.3.2. informações estatísticas de quantidade de conexões completadas e bloqueadas;

7.57.3.3. informações estatísticas de fluxo de tráfego e

7.57.3.4. informações estatísticas de quantidade de sessões ou conexões.

8. Serviços de Consolidação e Correlacionamento de Eventos:

Quantidade: 1

Meses de Prestação: 60 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de Consolidação e Correlacionamento de Eventos** deverão ser instalados no *datacenter* principal do TCU em Brasília, conforme desenho esquemático a ser obtido durante a vistoria prévia e no *datacenter* da contratada.

Os serviços deverão observar os seguintes requisitos mínimos:

8.1. providos com emprego de 2 (dois) elementos com função de consolidação e correlacionamento de eventos a serem instalados nos *datacenters* da contratada e 2 (dois) elementos com função de concentração de *logs*, a serem instalados em *rack* padrão 19" na sede do TCU (*datacenter* central) e no *datacenter* de contingência:

8.1.1. será admitida a utilização dos elementos com função de consolidação e correlacionamento de eventos em uso pela contratada para atender a outros contratos, desde que os requisitos sejam atendidos em partição exclusiva, com separação total de:

8.1.1.1. administração da ferramenta e respectivas contas de usuários;

8.1.1.2. configuração;

8.1.1.3. correlacionamento e

8.1.1.4. emissão de relatórios.

8.1.2. possui fonte de alimentação de 220V;

8.1.3. o conjunto dos requisitos especificados pode ser atendido por meio de outros equipamentos, produtos, peças ou *softwares*;

8.2. implementa alta disponibilidade com tolerância a falhas, sendo admitidas as configurações ativo-ativo ou ativo-passivo;

8.3. para os elementos com função de consolidação e correlacionamento de eventos, devem ser observadas as seguintes capacidades:

8.3.1. deve processar os eventos gerados por:

8.3.1.1. todos os equipamentos, produtos, peças ou *softwares* necessários à prestação dos serviços;

8.3.1.2. componentes do ambiente computacional do TCU, conforme tabela 2 a seguir:

Tabela 2 – Componentes do ambiente computacional do TCU

Ativo	Tipo/Marca	Quantidade
Sistema operacional	*Windows*	150
Sistema operacional	*Linux Red Hat*	50
Sistema operacional	*Cent OS*	20
Banco de dados	*Oracle*	5

Banco de dados	*SQL Server*	5
Banco de dados	*MySQL*	2
Servidor de aplicações	*JBoss*	10
Servidor de antivírus	*Symantec SEP*	2
Aplicação *WEB*	*Apache*	5
Aplicação *WEB*	*IIS*	5
Aplicação *WEB*	*Tomcat*	5
Roteadores	*Cisco*	35
Switches	*Enterasys*	50
Switches	*H3C*	3
Access Points	*3Com*	120
Switches Wireless	*3Com*	5
Aceleradores de tráfego *WAN*	*Riverbed*	35

8.4. para os elementos com função de concentração de *logs*, devem ser observadas as seguintes capacidades:

8.4.1. deve concentrar os *logs* gerados por:

8.4.1.1. todos os equipamentos, produtos, peças ou *softwares* necessários à prestação dos serviços;

8.4.1.2. componentes do ambiente computacional do TCU, conforme tabela 3 a seguir:

Tabela 3 – Componentes do ambiente computacional do TCU:

Ativo	Tipo/Marca	Quantidade
Sistema operacional	*Windows*	150
Sistema operacional	*Linux Red Hat*	50
Sistema operacional	*Cent OS*	20
Banco de dados	*Oracle*	5
Banco de dados	*SQL Server*	5
Banco de dados	*MySQL*	2
Servidor de antivírus	*Symantec SEP*	2
Servidor de aplicações	*JBoss*	10
Aplicação *WEB*	*Apache*	5
Aplicação *WEB*	*IIS*	5

Aplicação *WEB*	*Tomcat*	5
Roteadores	*Cisco*	35
Switches	*Enterasys*	50
Switches	*3Com*	150
Switches	*H3C*	3
Access Points	*3Com*	120
Switches Wireless	*3Com*	5
Aceleradores de tráfego *WAN*	*Riverbed*	35

8.5. permite a consulta aos alarmes e *logs* recebidos com e emitir relatórios, em ambos os casos utilizando os filtros abaixo:

8.5.1. origem do alarme (fonte do *log*);

8.5.2. endereço de origem do pacote que gerou o alarme;

8.5.3. endereço de destino do pacote que gerou o alarme;

8.5.4. tipo de alarme;

8.5.5. *string* de texto livre em qualquer campo dos *logs*;

8.5.6. categoria do *log*;

8.5.7. período de tempo e

8.5.8. rede *IP*.

8.6. o tempo de retenção dos *logs* gerados deverá ser equivalente ao prazo da vigência contratual;

8.7. no elemento com função de concentração de *logs* instalado no *datacenter* central o meio de armazenamento de *logs* deverá ser de 3 (três) meses *on-line* em equipamentos de armazenamento (*storage*) alocados pela contratada e instalados no ambiente do *datacenter* central do TCU;

8.8. no elemento com função de concentração de *logs* instalado no *datacenter* de contingência o tempo de retenção de *logs* deverá ser de 1 (hum) mês *on-line* em equipamentos de armazenamento (*storage*) alocados pela contratada e instalados no ambiente do *datacenter* de contingência do TCU;

8.9. a *media* (fita ou outro meio de armazenamento) contendo os *logs* mensais deverão ser entregues ao TCU, na reunião periódica, devendo compreender todos os *logs* do período de faturamento;

8.10. caso o TCU não possua facilidades de *software* e *hardware* para efetuar a leitura das *medias* entregues, estes leitores devem ser alocados pela contratada;

8.11. ao final do contrato, a contratada não deverá ficar com nenhuma copia dos *logs*, devendo entregar as *medias* utilizadas ao TCU;

8.12. integra a solução de consolidação e correlacionamento de eventos e de concentração de *logs* com o ambiente operacional do TCU;

8.13. suporta a configuração do agente de envio para mais de um coletor;

8.14. define e implementa regras de correlação, políticas e procedimentos adaptados ao ambiente do Tribunal;

8.15. desenvolve políticas e processos de manutenção de *logs* para as fontes, bem como procedimentos e processos de revisão;

8.16. planeja e implementa a arquitetura de gerenciamento de *logs* de acordo com o ambiente analisado, desenvolvendo filtros, formas de agregação, retenção e configuração das fontes;

8.17. define, planeja e implementa o recebimento de *logs* originados nas fontes monitoradas;
define, planeja e implementa o recebimento a busca dos *logs* nas fontes monitoradas que não enviem *logs* automaticamente;

8.18. correlaciona *logs* de eventos de diferentes dispositivos de segurança e infraestrutura de redes em tempo real;

8.19. analisa os *logs* recebidos e, com base nesta análise, aplica as melhores práticas relacionadas à manutenção e revisão de *logs*, de acordo com as políticas e normas do Tribunal;

8.20. todos os elementos sob responsabilidade da contratada, que enviem *logs* para este serviço, devem ser sincronizados por meio de protocolo *NTP*;

8.21. permite a configuração de *backups* programados da base de dados;

8.22. suporta customização para armazenar qualquer fonte de informação e formato de "*log*";

8.23. suporta *logs* de *event viewer*, *txt* e de *syslog*;

8.24. customiza os *logs* enviados pelas fontes;

8.25. armazena *logs* em seu estado cru, para fins de auditoria;

8.26. disponibiliza console de acesso aos eventos correlacionados para que a equipe de servidores designados pelo TCU efetue a visualização do *dashboard*, alarmes e correlações;

8.27. deve ser alimentado, mesmo que manualmente, com dados obtidos em:

8.27.1. bases de conhecimento sobre atividades anômalas na Internet (origens de ataques, protocolos etc), permitindo a correlação dinâmica dessas informações com os dados coletados na rede local;

8.27.2. bases de conhecimento contendo informações sobre vulnerabilidades e sugestões de remediação, apresentando os artigos relevantes ao incidente que está sendo analisado;

8.27.3. bases de conhecimento contendo listas de *IPs* maliciosos e *IPs* de *BotNet* que forem detectados na *Internet*, e utiliza esta informação como parte da correlação de eventos;

8.27.4. políticas adotadas ou elaboradas pelo TCU, permitindo correlacionar o evento e determinar a sua relevância em relação às políticas e, ainda, fornecer relatórios com a verificação de conformidade com aquelas políticas;

8.28. possui módulo centralizador para coleta e gestão das evidências de conformidade com políticas, *frameworks* e normas, inclusive gerando informações sobre violações identificadas;

8.28.1. informa ao TCU, em periodicidade a ser definida na reunião de *kick-off,* todos os ativos com identificação de não conformidade em relação às políticas, *frameworks* e normas que foram identificados durante a execução do contrato;

8.28.2. tais informações devem ser utilizadas na correlação e análise de eventos de forma a subsidiar a identificação de "falso positivo" e a priorização no tratamento dos *tickets*;

8.29. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7 e *Windows* XP, atendendo aos seguintes requisitos:

8.29.1. permite a replicação de configurações e a aplicação de atualização de *softwares* para todos os elementos que compõe este serviço;

8.29.2. permite a definição de diferentes níveis de administração, sendo, no mínimo, um nível completo e outro somente de visualização de configurações e *logs*;

8.29.3. permite a geração das seguintes informações, por período e elemento:

8.29.3.1. auditoria detalhada das alterações de configuração efetuadas, indicando usuário, ação e horário;

8.29.3.2. informações estatísticas de quantitativo de ataques identificados por tipo.

9. Serviços de Gestão de Vulnerabilidades:

Quantidade: 1

Meses de Prestação: 56 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de Gestão de Vulnerabilidades** deverão ser instalados no *datacenter* principal do TCU em Brasília, conforme desenho esquemático a ser obtido durante a vistoria prévia.

Os serviços deverão observar os seguintes requisitos mínimos:

9.1. providos com emprego de 1 (um) elemento com função de gestão de vulnerabilidades, para ser fixado em *rack* padrão 19”*;*

9.2. atualiza automaticamente a tabela de ativos do gerenciador de incidentes (ferramenta de gerência de chamados), preenchendo informações sobre os serviços e as vulnerabilidades encontradas no ativo analisado;

9.3. possui fonte de alimentação 220V;

9.4. oferece varredura “segura” de sistemas *SCADA – Supervisory Control and Data Acquisition*;

9.5. correlaciona eventos baseados nos sistema operacional, Porta/Protocolo, *Banners* e vulnerabilidades;

9.6. detecta vulnerabilidades em aplicações baseadas em *WEB*, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

9.7. verifica vulnerabilidades em ambiente *Windows* para, no mínimo: detecção de *hot fixes*, *service packs*, registros, *backdoors*, *trojans, malwares*, *peer to peer,* portas de serviço habilitadas e antivírus;

9.8. efetua descoberta de topologia dos ativos da rede (qualquer servidor ou ativo de rede que possua endereço IP ou que seja alocado no escopo desta contratação);

9.9. efetua varredura à procura de vulnerabilidades e *exploits*;

9.10. detecta vulnerabilidades em dispositivos de redes sem fio, aplicações baseadas em *WEB*, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

9.11. efetua descoberta das vulnerabilidades para os equipamentos, produtos, peças ou *softwares* alocados para atender aos requisitos de todos os itens de serviço e para todo o ambiente computacional do TCU escopo deste projeto, conforme Tabela 4, com frequência definida no tópico IV – Nível Mínimo de Serviços:

Tabela 4 – Componentes do ambiente computacional do TCU

Ativo	Tipo/Marca	Quantidade
Sistema operacional	*Windows*	150
Sistema operacional	*Linux Red Hat*	50
Sistema operacional	*Cent OS*	20
Banco de dados	*Oracle*	5
Banco de dados	*SQL Server*	5
Banco de dados	*MySQL*	2
Servidor de aplicações	*JBoss*	10
Aplicação *WEB*	*Apache*	5
Aplicação *WEB*	*IIS*	5

Aplicação *WEB*	*Tomcat*	5
Roteadores	*Cisco*	35
Switches	*Enterasys*	50
Switches	*3Com*	150
Switches	*H3C*	3
Access Points	*3Com*	120
Switches Wireless	*3Com*	5
Aceleradores de tráfego *WAN*	*Riverbed*	35
Imagem padrão para estações de trabalho	*Windows*	10

9.12. para executar a análise, deverá:

9.12.1. utilizar listas de vulnerabilidades da *SANS/FBI* e *IAVA* (*Information Assurance Vulnerability Alert*) ou possuir catalogado em suas bases mais de 50 (cinqüenta) mil vulnerabilidades;

9.12.2. integrar-se com base de dados de vulnerabilidades *CVE*;

9.12.3. possuir módulos de varredura diferenciados para análise intrusiva e não intrusiva;

9.12.4. analisar aplicações web para detecção de vulnerabilidades, tais como *Cross-Site-Scripting*;

9.12.5. efetuar varredura por endereço *IP*, Sistema Operacional, nome *DNS*, nome *NetBIOS* ou nome do domínio;

9.12.6. deve ser possível filtrar a varredura por:

9.12.6.1. destino;

9.12.6.2. serviço ou

9.12.6.3. vulnerabilidade.

9.13. inclui mecanismos para varredura de vulnerabilidades de *hosts*, bancos de dados e aplicações *web*, incluindo a detecção de vulnerabilidades em *AJAX* e *WEB* 2.0;

9.13.1. verifica vulnerabilidades:

9.13.1.1. de uma forma não invasiva;

9.13.1.2. por tipo de risco;

9.13.1.3. categoria;

9.13.1.4. por comparação de bases *CVE (Common Vulnerabilities and Exposures);*

9.14. analisa aplicação *WEB* a procura de informações em comentários *HTML*, *hyperlinks*, endereços de correio, *keywords*, campos escondidos e *scripts*;

9.15. identifica vulnerabilidades em *queries SQL* de aplicações *WEB,* suscetíveis a *SQL injection*;

9.16. analisa esquema de autenticação *WEB*;

9.17. apresenta pontuação que permite medir o nível de risco dos sistemas e dos recursos de rede TCU;

9.18. efetua levantamento e classificação quanto à criticidade de todos os ativos protegidos;

9.19. apresenta o nível de criticidade de cada ativo, indicando seu grau de exposição a *worms, exploits* e *malwares* em geral;

9.20. possui capacidade de configurar a velocidade da varredura de forma a não impactar a desempenho da rede;

9.21. gera alertas com informações detalhadas sobre o nome da vulnerabilidade, descrição detalhada, hosts afetados incluindo endereço IP e nome comum, os serviços abertos no host e as vulnerabilidades afetadas;

9.22. informa e avalia periodicamente a vulnerabilidade do Tribunal a eventuais falhas de segurança dos componentes de seu ambiente de TI, com o objetivo de indicar atualizações ou procedimentos necessários para eliminar ou mitigar as vulnerabilidades;

9.23. realiza periodicamente procedimentos ou atualizações necessários para mitigar vulnerabilidades dos componentes da solução de segurança;

9.24. corrige quaisquer vulnerabilidades detectadas na solução de segurança fornecida;

9.25. aplica solução de contorno, utilizando recursos da solução fornecida, a quaisquer vulnerabilidades detectadas no ambiente computacional monitorado;

9.26. apresenta os passos necessários para a realização da remediação das vulnerabilidades encontradas (inclusive instruções para aplicação de correções em produtos de terceiros).

9.27. analisa o ambiente de TI do Tribunal e, com base nesta análise, executa os seguintes procedimentos:

9.27.1. propõe a aplicação de melhores práticas à solução de segurança fornecida e melhorias na topologia utilizada pelo Tribunal;

9.27.2. sugere melhorias de segurança de forma a minimizar a exploração de vulnerabilidades;

9.28. a cada instalação de novo ativo ou mudanças em ativos existentes no parque monitorado, inclusive na imagem padrão para as estações de trabalho, deverá ser feita a análise de vulnerabilidades;

9.29. disponibiliza relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição dos ativos do TCU aos riscos identificados com, pelo menos, as seguintes informações:

9.29.1. nível de risco por plataforma e por vulnerabilidade;

9.29.2. sumário;

9.29.3. *score* com o nível de risco;

9.29.4. topologia de rede descoberta;

9.29.5. *hosts* descobertos;

9.29.6. serviços descobertos;

9.29.7. vulnerabilidades encontradas;

9.29.8. vulnerabilidades em *Windows*;

9.29.9. vulnerabilidades em aplicações *WEB*;

9.30. executa auditorias do ambiente utilizando os dados coletados e registrados na base de dados;

9.31. permite o gerenciamento de *baselines* de configuração dos ativos, que podem ser comparados com as novas avaliações para a determinação de desvios e envia alertas por *e-mail*;

9.32. suporta verificação de configurações e permissões nas plataformas de sistemas operacionais, bases de dados e correio eletrônico, para:

9.32.1. *Windows;*

9.32.2. *Unix Red Hat;*

9.32.3. Oracle;

9.32.4. SQL *Server* e

9.32.5. *Exchange*;

9.33. é administrado por ferramenta com interface gráfica remota segura, a partir de plataforma *Windows* 7, *Windows XP* ou interface *WEB*, e permite a definição de diferentes níveis de administração, no mínimo, um nível completo e outro somente de visualização de configurações e *logs.*

10. Serviços de Monitoração e Administração de Segurança:

Quantidade: 1

Meses de Prestação: 60 meses

Os equipamentos, produtos, peças ou *softwares* necessários à prestação dos **Serviços de Monitoração e Administração de Segurança** poderão ser instalados nos *datacenters* principal e de contingência do TCU em Brasília e nas dependências da contratada.

Os serviços deverão observar os seguintes requisitos mínimos:

10.1. serão realizados em todos os equipamentos, produtos, peças ou *softwares* alocados para atender aos requisitos de todos os itens de serviço, em regime 24x7 (24 horas por dia, sete dias por semana);

10.2. caso houver elementos instalados nas dependências do TCU, estes devem:

10.2.1. possuir fonte de alimentação 220V;

10.2.2. ser fixados em *rack* padrão 19";

10.3. executa as ações necessárias à resposta aos incidentes de segurança identificados de forma a manter os serviços disponíveis e operacionais;

10.4. mapeia e executa os processos de resposta dos incidentes de segurança ocorridos e documenta na base de conhecimento do Tribunal;

10.5. efetua a manutenção das regras e políticas do parque monitorado para responder a incidentes, à exceção dos ativos sob gestão exclusiva do TCU, cujos incidentes ou resultados de monitoração devem ser informados ao TCU;

10.6. verifica, diariamente, a disponibilização, pelo fabricante, de *patches*, correções e versões ou *releases* mais recentes dos *softwares*;

10.6.1. comunica ao TCU a existência do *patch* juntamente com os respectivos problemas resolvidos e as novas funcionalidades disponibilizadas. A periodicidade dessa comunicação será definida pelo TCU na reunião de início do projeto (*kick-off*);

10.7. atualiza os módulos da solução, isto é, fornece e instala *patches*, correções e versões ou *releases* mais recentes dos *softwares*;

10.8. executa procedimentos, resolve problemas e esclarece dúvidas relacionadas com instalação, configuração, atualização, funcionamento e uso dos equipamentos necessários ao funcionamento dos módulos;

10.9. executa atividades de gestão, suporte, manutenção, administração e resolução de problemas, mudanças de regras e de configuração, de cada um componentes dos serviços, remotamente ou *on-site*;

10.10. faz o ajuste fino (*tunning*) de toda a solução, adequando-a ao ambiente do Tribunal e às customizações de configuração necessárias para atender às necessidades do TCU;

10.11. resolve problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos equipamentos componentes da solução;

10.12. monitora os sites *WEB* do TCU contra pichação (*defacement*) e ataques, tais como cross-site scripting, SQL injection e DoS;

10.13. monitora servidores e alerta para mudança em arquivos de configuração;

10.14. executa inventários contendo as informações abaixo:

10.14.1. tipo de computador: servidor, estação ou outra classificação;

10.14.2. sistema operacional;

10.14.3. *service pack* aplicado;

10.14.4. *MAC Address;*

10.14.5. portas *TCP* e *UDP* ativas*;*

10.15. serão considerados incidentes de segurança qualquer ação que vise comprometer a integridade, a confidencialidade das informações ou a disponibilidade dos serviços de tecnologia da informação do TCU, tais como:

10.15.1. acessos indevidos;

10.15.2. instalação de códigos maliciosos;

10.15.3. indisponibilidade dos serviços (*DoS* e *DDoS*);

10.15.4. ataques por força bruta;

10.15.5. exploração de vulnerabilidades.

10.16. a monitoração deve utilizar canais de dados *WAN* próprios e redundantes, com tolerância a falhas, alocados no escopo da contratação, *out-of-band* (sem utilizar recursos de rede *WAN* do TCU), dedicado a este fim, conectando a "Rede TCU" à "Rede de Gerência" e à "Rede de Monitoração" da contratada, com acesso restrito e por meio de conexão segura e criptografada;

10.16.1. será permitida a prestação dos serviços por meio de:

10.16.1.1. estabelecimento de *VPN* em links *Internet* alocados pela contratada exclusivamente para essa conexão ou

10.16.1.2. estabelecimento de *VPN* em links *SLDD* alocados pela contratada exclusivamente para essa conexão;

10.16.1.3. caso seja necessária a utilização de elementos adicionais para o estabelecimento da *VPN*, estes devem ser alocados pela contratada.

10.16.2. o primeiro *link* deve interligar o *datacenter* central ao *SOC* principal, ou estabelecer a *VPN* entre eles;

10.16.3. o segundo *link* deve interligar o *datacenter* de contingência no TST ao *SOC* de contingência, ou estabelecer a *VPN* entre eles;

10.16.4. no caso de utilizar link *Internet*, devem ser utilizados no *SOC*, 02 (dois) canais de comunicação *IP* dedicados com provedores distintos, para a prestação de serviços de monitoramento e suporte remoto. Não serão aceitos contratos com *links xDSL* (excetuada a tecnologia *HDSL)*;

10.17. avalia periodicamente a customização dos *softwares* de gerência da contratada, incluindo os alarmes de todos os componentes da e ajusta as suas configurações, de maneira que ocorrências de problemas, incidentes ou irregularidades sejam devidamente notificadas no console de gerência;

10.18. é possível o acesso remoto a interface de monitoramento;

10.19. executa a gestão estratégica de cada equipamento ou *software* utilizado na solução, monitorando a utilização de *CPU*, memória e demais recursos monitoráveis, de forma a construir *baseline* com informações de, pelo menos, 3 (três) meses;

10.20. é feita a partir de Centros de Operações de Segurança (*SOC*) redundantes, localizados no Brasil, de modo que a indisponibilidade de um deles não afete nenhum aspecto

dos serviços prestados. Será admitida a utilização do segundo *SOC* em ambiente físico terceirizado, fora das dependências da contratada, desde que os serviços sejam prestados por funcionários da contratada;

10.21. ambos os *SOCs* devem atender aos mesmos requisitos, a saber:

10.21.1. utiliza sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da contratada e cujas imagens possam ser recuperadas;

10.21.2. filma toda a área, mantendo as imagens armazenadas por 90 (noventa) dias;

10.21.3. efetua registro de entrada e saída dos visitantes, com identificação individual, em todos os acessos ao *SOC*;

10.21.4. possui solução de monitoramento de disponibilidade e desempenho em seu Centro de Operações de Rede e Segurança;

10.21.5. caso os serviços de gerenciamento e monitoramento não sejam feitos no mesmo espaço físico que o *SOC*, todos as requisitos devem ser atendidos em todos os locais de prestação desses serviços;

10.21.6. o perímetro do *SOC* é equipado com sensor de intrusão e alarmes contra acesso indevido;

10.21.7. é vigiado de forma ininterrupta por segurança especializada em regime de 24x7x365;

10.21.8. o controle de acesso físico ao ambiente do *SOC* deve ser construído com pelo menos 2 (dois) fatores de autenticação.

10.22. os ativos de TI empregados no monitoramento, como servidores, appliances, equipamentos, softwares etc., excetuando-se as estações de trabalho, devem atender aos seguintes requisitos:

10.22.1. possui sistemas redundantes para armazenamento de dados e alimentação de energia;

10.22.2. possui estrutura de armazenamento de dados que permita a manutenção dos registros dos eventos relacionados aos serviços contratadas por, no mínimo, o prazo do contrato;

10.22.3. configurado de forma que a falha de um dos equipamentos isoladamente NÃO interrompa a prestação dos serviços;

10.22.4. estar hospedado em dois *datacenters* diferentes, localizados no Brasil, de forma que a falha completa de um dos *datacenters* não afete a prestação dos serviços. Cada um dos *datacenters* deve possuir:

10.22.4.1. sistema de gerenciamento de CFTV, que viabilizem o rastreamento de pessoas dentro do ambiente da contratada e cujas imagens possam ser recuperadas;

10.22.4.2. filmagem de toda a área mantendo as imagens armazenadas por 90 (noventa) dias;

10.22.4.3. registro de entrada e saída dos visitantes com identificação individual;

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

10.22.4.5. sistema de provimento ininterrupto de energia elétrica, composto por grupo gerador e *UPSs* para garantir a transição entre o fornecimento normal de energia e o grupo gerador;

10.22.4.6. piso elevado e sistema de cabeamento estruturado categoria 6;

10.22.4.7. mecanismos automáticos de extinção de fogo por agentes gasosos não poluentes do tipo *FE227 ou FM200*;

10.22.4.8. componentes de segurança necessários para garantir a preservação dos dados em casos de incêndio e execução de plano de recuperação de catástrofes;

10.22.4.9. integração com sistema de alarme e ser monitorado em tempo integral e

10.22.4.10. sistemas redundantes com disponibilidade de equipamentos igual a N+1.

10.22.5. os *Datacenters* podem estar situados no mesmo ambiente que o SOC;

10.23. executa atividades de manutenção e configuração da solução contratada, que deverão ocorrer de acordo com o Processo de Gerenciamento de Mudanças adotado pelo TCU;

10.24. alimenta o sistema do TCU para o processo de Gestão de Mudanças, atualmente é utilizado o *CA Service Desk*;

10.25. protege servidores contra ataques *zero-day* por meio de políticas comportamentais, sem a necessidade de atualização da base de assinaturas;

10.26. efetua proteção dos servidores executando ações como controle de acesso a processos, por *IP* ou porta.

11. Treinamento:

A contratada deverá disponibilizar, sob demanda, serviços de treinamento especializado em segurança da informação, de forma a atender aos seguintes requisitos:

11.1. A contratada deverá realizar treinamento para os itens de serviço abaixo:

11.1.1. Serviços de *Firewall* Central Externo;

11.1.2. Serviços de *Firewall* e *VPN* Central Interno;

11.1.3. Serviços de *Firewall* e *VPN* Remoto;

11.1.4. Serviços de Prevenção de Intrusão Central;

11.1.5. Serviços de *Proxy/cache* com filtro de conteúdo *WEB*;

11.1.6. Serviços de *SMTP Antispam*;

11.1.7. Serviços de *Firewall* de Aplicação;

11.1.8. Serviços de Consolidação e Correlacionamento de Eventos;

11.1.9. Serviços de Gestão de Vulnerabilidades;

11.1.10. Serviços de Monitoração e Administração de Segurança;

11.2. deverá ser provido em módulos, ao final de cada uma das etapas de instalação;

11.3. cada módulo terá até 10 (dez) participantes;

11.4. a duração mínima de cada treinamento obedecerá a Tabela 5 a seguir:

Tabela 5 – Carga horária mínima de treinamentos

Item	Carga horária mínima
Serviços de *Firewall* Central Externo	20h/a
Serviços de *Firewall* e *VPN* Central Interno	20h/a
Serviços de *Firewall* e *VPN* Remoto	16h/a
Serviços de Prevenção de Intrusão Central	12h/a
Serviços de *Proxy*/*cache* com filtro de conteúdo *WEB*	12h/a
Serviços de *SMTP Antispam*	12h/a
Serviços de *Firewall* de Aplicação	20h/a
Serviços de Consolidação e Correlacionamento de Eventos	12h/a
Serviços de Gestão de Vulnerabilidades	8h/a
Serviços de Monitoração e Administração de Segurança	8h/a

11.5. caso os serviços objeto dos itens 1, 2 e 3 sejam providos com emprego de tecnologias equivalentes, de mesmo fabricante, os treinamentos objeto dos itens 11.1 e 11.3, a critério do TCU, poderão não ser executados;

11.6. o conteúdo do treinamento deverá ser de natureza teórica e prática, devendo abranger todos os equipamentos, componentes e *softwares* dos módulos alocados, em seus aspectos mais relevantes e, em especial, envolvendo aqueles relacionados à solução implantada no ambiente computacional do Tribunal, contendo, no mínimo:

11.6.1. apresentação do projeto implementado;

11.6.2. descrição da arquitetura física e lógica de cada equipamento;

11.6.3. descrição do *hardware* e *software* de cada equipamento;

11.6.4. estratégias de implementação dos equipamentos;

11.6.5. configuração e administração dos equipamentos;

11.6.6. descrição geral da plataforma de gerência;

11.6.7. diagnóstico de problemas;

11.6.8. configuração de alarmes para os serviços de monitoramento;

11.6.9. configuração de eventos para os serviços de monitoramento;

11.6.10. configuração de rotinas de coleta de dados para monitoramento;

11.6.11. gerência de desempenho e segurança;

11.6.12. manipulação de objetos *MIB, SNMP* e *RMON* para monitoração;

11.6.13. resolução de problemas ("*troubleshooting*");

11.6.14. gestão de mudanças e configuração;

11.6.15. relatórios de acesso;

11.7. condições de execução dos treinamentos:

11.7.1. deverão ser previamente agendados pelo TCU por meio de Ordem de Serviço de Treinamento, conforme modelo definido no Anexo VI do Edital do Pregão Eletrônico n.º 86/2011, em comum acordo entre o Tribunal e a contratada;

11.7.2. a alteração dos prazos de início/término do treinamento definidos na respectiva Ordem de Serviço de Treinamento somente será possível mediante apresentação, pela contratada, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pelo Tribunal;

11.7.3. as ordens de serviço de treinamento só serão consideradas concluídas após a avaliação do treinamento realizado ser feita pelo TCU;

11.7.4. estando todos os elementos necessários, o Tribunal fará o recebimento definitivo dos treinamentos no prazo máximo de 15 (quinze) dias úteis contados do fim do treinamento;

11.7.5. para a recebimento definitivo será preenchido o Termo de Recebimento de Serviços de Treinamento, conforme modelo definido no Anexo VII do Edital do Pregão Eletrônico n.º 86/2011;

11.7.6. a contratada deverá providenciar material didático individual que abranja todo o conteúdo do curso. Não será exigido material oficial do fabricante, entretanto este será avaliado pela equipe técnica do TCU antes da realização do curso, e caso seja considerado insuficiente, deverá ser readaptado para as condições exigidas pelo Tribunal;

11.7.7. devem ser observados os seguintes requisitos e prazos:

11.7.7.1. caso não seja utilizado treinamento padrão do fabricante, uma versão do material didático deve ser encaminhada, para avaliação prévia, com antecedência mínima de 20 (vinte) dias úteis da data para o início do treinamento, indicada na respectiva ordem de serviço de treinamento;

11.7.7.2. o TCU deve avaliar o material em até 5 (cinco) dias úteis, contados da data do recebimento do mesmo;

11.7.7.3. a contratada deverá reapresentar o material corrigindo eventuais observações feitas pelo TCU em até 10 (dez) dias úteis, contados da data de notificação efetuada pelo Tribunal;

11.7.7.4. a cada remessa para avaliação pelo TCU, a equipe para análise do material didático será designada pelo titular da ***Diretoria de Gestão do Ambiente Computacional – Diamb/Setic*** e terá prazo de até 5 (cinco) dias úteis para efetuar a análise do respectivo material***;***

11.7.7.5. caso o TCU avalie o material corrigido como insuficiente ou inadequado, a contratada será considerada em atraso até que sejam sanadas todas as pendências;

11.8. para a consecução da parte prática do treinamento, deverão ser utilizados equipamentos similares aos ofertados, além de todos os *softwares* que fizerem parte da solução;

11.9. o treinamento deverá ser realizado em Brasília-DF, em instalações fornecidas pela contratada, em horário comercial, sendo limitado a 4 (quatro) horas/aula diárias;

11.10. o treinamento deverá ser realizado em dias consecutivos, salvo se expressamente autorizado pelo TCU;

11.11. o período e horário de realização do curso deverão ser definidos pela contratada, em conjunto com o Tribunal, para momento posterior ao recebimento definitivo do respectivo item de serviço;

11.12. os instrutores deverão possuir qualificação técnica compatível com a solução, que deverá, no momento da assinatura da ordem de serviço de treinamento, ser demonstrada por, pelo menos, dois dos documentos abaixo relacionados:

11.12.1. certificação no produto (no caso de utilizar algum produto em *software* livre, o instrutor deve possuir a certificação LPI;

11.12.2. realização de curso oficial do fabricante;

11.12.3. experiência comprovada de 5 (cinco) anos na tecnologia.

11.13. a contratada deverá fornecer, ao final do curso, certificado individual de conclusão com aproveitamento do curso;

11.14. o TCU se reserva no direito de exigir que qualquer treinamento seja ministrado novamente com alterações, caso não seja considerado satisfatório pela equipe de análise do material didático, anteriormente designada pelo titular da ***Diretoria de Gestão do Ambiente Computacional – Diamb/Setic*** para tal fim.

12. Serviços Técnicos Especializados:

Quantidade: 1.600 horas

A contratada deverá disponibilizar, sob demanda, horas de serviços técnicos especializados em segurança da informação, de forma a atender aos seguintes requisitos:

12.1. execução de até 1.600 (um mil e seiscentas) horas;

12.1.1. é prevista a utilização média de 320 horas por ano;

12.1.2. não há garantia de execução das 1.600 horas, trata-se apenas de previsão estimativa;

12.2. os serviços elegíveis a serem executados limitar-se-ão, exclusivamente, aos seguintes casos:

12.2.1. elaboração de pareceres em segurança da informação;

12.2.2. análise de segurança em elementos que não sejam de propriedade da contratada ou que não estejam no escopo desse projeto;

12.2.3. suporte aos planos de melhoria na infraestrutura de segurança do TCU;

12.2.4. suporte a mudanças de arquitetura do ambiente do TCU, sobretudo aos aspectos de segurança envolvidos;

12.2.5. avaliação de vulnerabilidades da rede do Tribunal fora do escopo desse projeto, incluindo a indicação de atualizações ou procedimento necessários para mitigá-las;

12.2.6. apoio na definição e implementação de mecanismos futuros de monitoramento de segurança;

12.2.7. configuração de segurança e atualização de versão de *softwares* de equipamentos de rede, excluídos os equipamentos de propriedade da contratada;

12.2.8. orientação quanto a procedimentos de auditoria forense no ambiente computacional do TCU;

12.2.9. elaboração, em conjunto com o TCU, de planos de conscientização de usuários que proporcionem maior grau de segurança;

12.2.10. mudanças de endereço:

12.2.10.1. incluem-se no escopo dos serviços a desinstalação, o transporte para o novo endereço e a reinstalação de todos os equipamentos, produtos, peças ou *softwares* necessários à prestação dos serviços;

12.2.10.2. excetuam-se do escopo dos **Serviços Técnicos Especializados** as mudanças de endereço do *datacenter* central para o *datacenter* de contingência, para os elementos que compõem *clusters*, previstas neste Termo, que deverão ser executadas sem ônus adicional ao Tribunal,

12.2.11. transferência de conhecimento às pessoas indicadas pelo TCU (até dez pessoas por evento), por meio de *workshops*, conforme as características abaixo:

12.2.11.1. ser realizado em Brasília, nas dependências do TCU;

12.2.11.2. ter duração máxima de 3 (três) horas;

12.2.11.3. ter como conteúdo os conhecimentos referentes a operação, administração, procedimentos e incidentes ocorridos e respectivas ações de mitigação, problemas vivenciados e soluções aplicadas e mudanças de arquitetura ou de tecnologia, além de informações necessárias à transição contratual.

12.3. não serão passíveis de execução por meio de utilização dos **Serviços Técnicos Especializados** as atividades elencadas nos demais itens e tópicos deste Anexo;

12.4. para a execução dos serviços especificados neste item, a contratada deverá alocar pelo menos um profissional que detenha uma das qualificações abaixo, a ser comprovada no momento da assinatura da ordem de serviço:

12.4.1. certificação no produto objeto dos serviços ou

12.4.2. experiência comprovada de 5 (cinco) anos na tecnologia objeto dos serviços;

12.5. condições de execução dos serviços:

12.5.1. os serviços serão executados nas instalações do Tribunal de Contas da União e do TST, por técnicos da empresa contratada detentores do perfil adequado. Entretanto, será possível a execução dos serviços fora das instalações do Tribunal, desde que previamente autorizado pelo Tribunal;

12.5.2. os serviços serão executados em Brasília, com exceção daqueles definidos no item 12.2.10;

12.5.3. quaisquer serviços ou procedimentos realizados deverão ser previamente aprovados pelo TCU por meio de Ordem de Serviço, conforme modelo definido no Anexo VIII do Edital do Pregão Eletrônico n.º 86/2011, em comum acordo entre o Tribunal e a contratada, sendo que o tempo necessário ao atendimento deverá ser previamente definido na respectiva Ordem de Serviço;

12.5.4. a prorrogação do prazo de execução de uma Ordem de Serviço somente será possível mediante apresentação, pela contratada, de relatório de impacto contendo justificativas plausíveis, devidamente aceitas pelo Tribunal, ou por interesse do TCU, em caso de impedimento devidamente justificado que dificulte ou não permita a execução dos serviços;

12.5.5. as ordens de serviço só serão consideradas concluídas após a entrega da documentação dos procedimentos e da configuração resultante nas bases e nos padrões definidos pelo TCU (incluindo documento *as-built*);

12.5.6. para recebimento dos serviços será preenchido o Termo de Recebimento de Serviços, conforme modelo definido no Anexo IX do Edital do Pregão Eletrônico n.º 86/2011.

12.5.6.1. o TCU deve avaliar os produtos entregues em até 10 (dez) dias úteis contados da entrega dos serviços/produtos exigidos;

12.5.6.2. a contratada deverá reapresentar o material corrigindo eventuais observações feitas pelo TCU em até 10 (dez) dias úteis, a contar da comunicação pelo TCU;

12.5.6.3. a cada remessa para avaliação pelo TCU, a equipe para análise dos produtos da Ordem de Serviço será designada pelo titular da ***Diretoria de Gestão do Ambiente Computacional – Diamb/Setic*** e terá prazo de até 10 (dez) dias úteis para análise dos produtos entregues;***;***

12.5.6.4. caso o TCU avalie o material corrigido como insuficiente ou inadequado, a contratada será considerada em atraso até que sejam sanadas todas as pendências;

12.5.7. estando todos os elementos necessários, o Tribunal fará o recebimento definitivo dos serviços no prazo máximo de 15 (quinze) dias úteis;

12.5.8. estando todos os elementos necessários, o Tribunal fará o recebimento definitivo da ordem de serviço no prazo máximo de 15 (quinze) dias úteis contados do recebimento dos serviços/produtos exigidos;

12.5.9. para a recebimento definitivo será preenchido o Termo de Recebimento de Serviços, conforme Anexo IX do Edital do Pregão Eletrônico n.º 86/2011.

12.5.10. o Tribunal somente autorizará o pagamento das faturas emitidas após o recebimento definitivo dos serviços, realizado mensalmente, de acordo com os níveis mínimos de serviço estabelecidos.

II. PLANEJAMENTO, CUSTOMIZAÇÃO DE AMBIENTE E INSTALAÇÃO DE ATIVOS DE REDE

A contratada deverá atender as seguintes condições gerais para início de prestação de cada um dos serviços, incluindo fase de concepção da solução, confecção de Projeto Executivo, planejamento de atividades de instalação, customização de ambiente, migração tecnológica e ativação de serviços, sem ônus adicionais ao TCU:

1. serão de responsabilidade da contratada as atividades de instalação, integração, configuração e testes de todos os produtos componentes de cada solução alocada, em conformidade com o Projeto Executivo a ser elaborado e apresentado pela contratada para aprovação pelo TCU;
2. caso os produtos alocados venham a substituir solução existente no TCU, caberá à contratada levantar a configuração atual e fazer a migração das configurações existentes para a solução utilizada no provimento dos serviços;

3. a contratada deverá levantar informações acerca dos locais de instalação dos produtos durante a elaboração do Projeto Executivo, e, se pertinente, efetuar visita técnica para verificar eventuais requisitos físicos a serem providos para a correta instalação e prestação dos serviços;

   3.1. as visitas poderão ser realizadas nos dia úteis, das 10:00h as 18:00h, mediante agendamento prévio com a unidade responsável (Sesti), por meio dos telefones (61)3316.5499 ou (61)3316.2489;

4. será necessária para a prestação dos serviços, a alocação de *racks* de rede para instalação dos equipamentos que comporão os itens 3 – Serviços de *Firewall* e *VPN* Remoto;

   4.1. os *racks* de 19" a serem alocados deverão ter porta com chave e ter capacidade mínima de 20 *U*'s ;

   4.2. serão necessários 10 (dez) *racks*, sendo que a contratada deverá avaliar previamente, em cada Secretaria Estadual de Controle Externo, as condições de espaço físico existentes em cada localidade, de forma a planejar a migração com máxima precisão;

   4.3. espaços ociosos desses *racks* poderão ser usados para a instalação de ativos de rede de propriedade do Tribunal.

5. Independentemente da alocação dos *racks* pela contratada, esta deverá efetuar a reorganização dos *racks* existentes, de forma a acomodar os seus equipamentos;

6. as atividades de migração deverão ocorrer de acordo com o Processo de Gerenciamento de Mudanças adotado pelo TCU:

   6.1. as reuniões de Gerenciamento de Mudanças são realizadas por meio de um Comitê de Mudanças (*Change Advisor Board – CAB*), com periodicidade semanal;

   6.2. o *CAB* é responsável por aprovar ou vetar mudanças no ambiente operacional que por ventura venham a causar indisponibilidade ou impactos no desempenho dos serviços de TI;

   6.3. do Comitê, participam servidores do Tribunal responsáveis pela disponibilização e manutenção da infraestrutura de TI do Tribunal;

   6.4. na ocasião das reuniões, poderá ser solicitada à contratada, com até 48 (quarenta e oito) horas de antecedência, a presença do técnico responsável pelas atividades de migração, para exposição dos riscos associados.

7. a elaboração do Projeto Executivo estará a cargo da contratada e deverá atender as seguintes condições:

   7.1. conter as fases do projeto, os cronogramas de execução e a descrição detalhada dos produtos e subprodutos a serem entregues em cada fase, respeitando o prazo máximo total de 12 (doze) meses para a entrega de todas as etapas previstas, a contar da assinatura do contrato;

   7.2. conter a descrição de topologia lógica e física da rede atual e topologia pretendida em cada etapa;

7.3. efetuar o mapeamento de criticidade de todos os ativos envolvidos no projeto, inclusive os de propriedade do TCU;

7.4. projetar a engenharia de tráfego da rede TCU;

7.5. planejar a migração das configurações do parque atualmente em funcionamento;

7.6. para implantação dos serviços, indicar de forma detalhada as condições de *rollback* de cada mudança no ambiente do TCU;

7.7. estimar o consumo de unidades de *rack* em *U*'s e de energia de cada ativo a ser instalado nas dependências do TCU;

7.8. detalhar a ementa dos treinamentos a serem ministrados;

8. os equipamentos, *softwares* e demais componentes necessários à correta prestação dos serviços deverão:

8.1. ser entregues, instalados e configurados nas dependências definidas pelo Tribunal de Contas da União, nos endereços indicados no item XIII – Local de Execução dos Serviços;

8.2. conter os recursos necessários e estarem configurados de modo a garantir total operabilidade no ambiente computacional do Tribunal, e otimizados para usufruir das melhores condições em termos de desempenho e disponibilidade;

8.3. conter a última versão de software e firmware disponibilizada pelo fabricante;

8.4. ter configuradas senhas de acesso para que a equipe de servidores designados pelo TCU efetue o acesso para a visualização das configurações e logs;

8.5. ter configurada senha com direitos totais de administração e configuração a ser utilizada pelo TCU em caso de emergência;

8.6. ser configurados para enviar *logs* para as soluções de concentração de *logs* disponibilizados no site central e de contingência do TCU;

8.7. ser configurados para gerenciamento *SNMP* versões 1 e 2 por meio da solução em uso pelo Centro de Operação de Redes do TCU. A plataforma atual consiste no *software Zabbix*;

9. todos os recursos para implantação dos serviços providos pela contratada serão por ela providenciados, sem ônus adicionais. Incluem-se, entre outros:

9.1. cabeamento de rede para interligação ao *switch core* da rede e demais ativos necessários ao funcionamento adequado da solução;

9.2. cabeamento de energia elétrica para alimentação dos equipamentos e respectivos adaptadores;

9.3. quaisquer materiais, cabos, parafusos, porcas, conectores elétricos, tomadas, adaptadores ou acessórios necessários ao cumprimento dos requisitos dos diversos serviços;

10. para aprovação da instalação e configuração de qualquer item que enseje a emissão de termo de recebimento definitivo, a contratada deve elaborar relatório técnico com análise dos resultados e impactos decorrentes da atividade executada;

11. as atividades quando realizadas no ambiente de produção poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 20h, ou em finais de semana e feriados. Há restrições para mudanças às terças-feiras, quartas-feiras e quintas-feiras);

12. a instalação será dividida em quatro etapas:

12.1. etapa I, composta dos seguintes serviços:

12.1.1. *Firewall* Central Externo, *Firewall* e *VPN* Central Interno, Consolidação e Correlacionamento de Eventos e Monitoração e Administração de Segurança para a Solução;

12.2. etapa II, composta dos seguintes serviços:

12.2.1. *Proxy/cache* com filtro de conteúdo *WEB* e *SMTP (Antispam);*

12.3. etapa III, composta dos seguintes serviços:

12.3.1. *Firewall* e *VPN* Remoto e Gestão de Vulnerabilidades;

12.4. etapa IV, composta dos seguintes serviços:

12.4.1. *Firewall* de Aplicação e Prevenção de Intrusão Central;

12.5. a instalação de uma etapa somente será iniciada após a finalização da etapa anterior;

12.5.1. entende-se por finalização o ato de:

12.5.1.1. submeter para recebimento definitivo o item de serviço após a customização e instalação de todos os elementos necessários à prestação dos serviços de cada fase;

12.5.1.2. entrega da documentação "*as-built*";

12.5.1.3. entrega da documentação comprobatória das licenças de uso de todos os *softwares* utilizados nos serviços finalizados;

12.5.1.4. entrega da documentação comprobatória da garantia do fabricante de todo o *hardware* necessário à prestação dos serviços de cada fase;.

12.5.1.5. entrega da documentação comprobatória do contrato de suporte técnico e atualização de versões do fabricante de todo o *software* e *hardware* necessário à prestação dos serviços de cada fase;.

12.5.2. não será admitida a instalação concorrente de serviços de fases distintas;

12.6. nos casos previstos neste edital, o Tribunal poderá solicitar a migração de elementos para o *datacenter* de contingência do TCU no TST, em Brasília;

12.6.1. após a solicitação do TCU, a contratada terá, no máximo, 15 dias para executar a migração;

12.6.2. todos os passos necessários para a consecução da atividade devem ter sido previstos no Projeto Executivo, inclusive com a determinação dos prazos necessários a cada etapa da migração;

13. após a instalação, a contratada deverá realizar operação assistida para os serviços abaixo:

13.1. *Firewall* Central Externo;

13.2. *Firewall* e *VPN* Central Interno;

13.3. *Firewall* e *VPN* Remoto;

13.4. Prevenção de Intrusão Central;

13.5. *Proxy*/*cache* com filtro de conteúdo *WEB*;

13.6. *SMTP Antispam*;

13.7. *Firewall* de Aplicação;

13.8. *Gestão de Vulnerabilidades.*

14. a operação assistida deverá obedecer aos requisitos abaixo:

14.1. iniciará quando forem finalizados o planejamento, a customização de ambiente e a instalação dos ativos de rede, sendo o item de serviço submetido para recebimento definitivo. A mudança para o ambiente de produção será concomitante a este momento, salvo se expressamente solicitado pelo TCU que seja feita em data diferente;

14.2. terá duração de 40 (quarenta) dias corridos para os serviços dos itens 4 – Prevenção de Intrusão Central e 7 – *Firewall* de Aplicação, sendo que durante os primeiros 20 (vinte) dias da operação assistida, os equipamentos deverão ser configurados apenas para monitorar a rede, sendo que a configuração para executar ações corretivas e preventivas deverá ser liberada após aprovação pelo TCU, durante os 20 (vinte) dias seguintes;

14.2.1. os prazos de monitoramento e de execução de ações preventivas poderá ser alterado desde que a duração total se mantenha em 40 (quarenta) dias;

14.3. para os demais itens terá duração de 20 (vinte) dias corridos;

14.4. será executada em Brasília, nas dependências do TCU, em horário comercial (10:00h às 19:00h);

14.5. caso seja necessária a consecução de atividades, pelo técnico responsável pela operação assistida, que possam afetar a disponibilidade de serviços de rede do TCU, estas devem ocorrer após as 20:00h;

14.6. caso o TCU encontre pendências impeditivas à emissão do termo de recebimento definitivo, a operação assistida deverá ser prorrogada até que sejam sanados os motivos geradores das pendências;

14.7. caso a implantação de um serviço cause interferência no funcionamento de qualquer funcionalidade da Rede TCU, a contratada deverá alocar profissionais com qualificação suficiente para corrigir o problema ou retornar o ambiente à condição anterior à implantação.

15. a contratada deverá implementar e documentar para todos os componentes da solução as configurações de segurança necessárias, que visem à redução do risco de acesso indevido a cada servidor (*hardening*), como, por exemplo, remoção de serviços desnecessários do sistema operacional, configurações de *kernel*, configurações dos serviços ativos para suas permissões mínimas de funcionamento, remoção de usuários-padrão de sistemas e aplicativos, além de eventuais configurações para resistir a ataques de negação de serviço.

III. REQUISITOS GERAIS PARA PRESTAÇÃO DOS SERVIÇOS

A contratada deverá observar aos seguintes requisitos mínimos gerais para a prestação dos serviços, sem ônus adicionais ao TCU:

1. a contratada deverá assinar o documento contido no Anexo IV – Termo de Confidencialidade e Sigilo da contratada do Edital do Pregão Eletrônico n.º 86/2011, e entregá-lo ao TCU com firmas reconhecidas em cartório, até a data marcada para a reunião de início de projeto. Consistem em condição para a prestação de todos os serviços, estabelecendo sigilo das informações do ambiente do Tribunal de Contas da União, com acesso mínimo e restrito aos técnicos designados para a prestação dos serviços:

   1.1. a contratada será responsável por obter as assinaturas nos respectivos termos de seus funcionários, terceirizados, parceiros ou quaisquer outras pessoas que venham executar serviços integrantes do objeto desta contratação;

   1.2. o Termo de Confidencialidade e Sigilo determina que a propriedade intelectual de todos os produtos ou conhecimentos gerados advindos da prestação dos serviços pertence ao TCU.

2. todos os equipamentos, produtos, peças ou *softwares* componentes dos serviços entregues deverão:

   2.1. ocupar nos respectivos *racks*, no máximo (a informação de ocupação de *U's* pela solução proposta pelo licitante deve constar na sua proposta comercial):

      2.1.1. 78 (setenta e oito) *U's* no *datacenter* central do Tribunal;

         2.1.1.1. após a mudança dos elementos previstos para o *datacenter* de contingência, a ocupação máxima será de:

2.1.1.1.1. 44 (quarenta e quatro) *U's* no *datacenter* central do Tribunal;

2.1.1.1.2. 34 (trinta e quatro) *U's* no *datacenter* de contingência do Tribunal;

2.1.2. 6 (seis) *U's* nos *sites* remotos do Tribunal, isto é, nas Secretarias de Controle Externo nos Estados e no Instituto Serzedello Correa;

2.2. no caso de serem instalados em *cluster:*

2.2.1. possuir mecanismos para evitar que ocorram situações conhecidas como "*split brain*";

2.2.2. na indisponibilidade de um dos nós do *cluster*, um único nó ativo deverá suportar todos os requisitos de desempenho e funcionalidades definidos nas especificações técnicas.

2.3. estar cobertos pela garantia do fabricante durante o período de vigência de cada um dos serviços, no caso de equipamentos, produtos e peças;

2.4. estar cobertos por contratos de suporte técnico e atualização de versões junto aos fabricantes durante o período de vigência de cada um dos serviços em que serão utilizados, no caso de *softwares* comerciais.

3. será admitida a utilização de equipamentos do tipo *UTM (Unified Threat Management)* para atendimento aos requisitos de prestação dos serviços, desde que:

3.1. o desempenho do produto atenda às exigências especificadas neste edital com todas as funcionalidades requeridas habilitadas;

3.2. os requisitos de desempenho e capacidade dos serviços atendidos pelo mesmo produto sejam somados;

3.3. se for utilizado um equipamento para atender simultaneamente aos itens relativos a *firewalls* e *IPS*, o *firewall/IPS* deverá ser capaz de:

3.3.1. selecionar os tipos de tráfego a ser enviado ao *IPS* e

3.3.2. a comunicação entre o *firewall* e o *IPS* deverá ser totalmente interna ao equipamento, sem necessidade de uso de qualquer interface externa.

3.4. para os equipamentos a serem instalados no *datacenter* central, cada funcionalidade deverá ser executada em um módulo de *hardware* dedicado com interface de gerência e interface de console dedicadas;

3.4.1. para atendimento ao item 4 (Serviços de Prevenção de Intrusão Central) será admitido o compartilhamento do mesmo módulo de *hardware* utilizado para executar as funcionalidades exigidas nos itens 1 (Serviços de *Firewall* Central Externo) e 2 (Serviços de *Firewall* e VPN Central Interno).

4. caso sejam utilizados *softwares* livres na solução fornecida, estes deverão observar aos seguintes requisitos:

4.1. serem de código aberto;

4.2. os pacotes deverão ser obtidos de repositórios de distribuidores oficiais ou compilados a partir do código-fonte obtido no site oficial de desenvolvimento;

4.3. deverão ser *aplicados* os patches e atualização de versão, obedecendo aos mesmos prazos definidos para os *softwares* comerciais;

4.4. deverão possuir comunidades de suporte consolidadas e estruturadas.

5. todos os recursos necessários à configuração e administração dos equipamentos, *softwares* ou quaisquer outros componentes da solução fornecida deverão ser instalados no TCU e estar disponíveis mesmo com a perda de comunicação com a central de monitoramento e gerência da contratada;

6. quaisquer agentes ou certificados digitais necessários à perfeita consecução dos serviços devem ser alocados pela contratada, sem ônus adicional ao TCU;

7. a contratada assumirá inteira responsabilidade por danos ou desvios eventualmente causados ao patrimônio do TCU ou de terceiros por ação ou omissão de seus empregados ou prepostos, quando tenham sido causados por seus profissionais durante a execução dos serviços;

8. a contratada deverá adotar mecanismos para proteger os equipamentos que fazem parte do escopo da solução fornecida contra roubo, furto e danos;

9. nos equipamentos do tipo “servidor” necessários à correta prestação dos serviços deverão ser instalados produtos *antivírus* com serviço de recebimento do banco de dados de assinaturas ativo, durante toda a vigência do contrato;

10. caso o TCU julgue pertinente, poderá ser requisitada, sem ônus adicional, a permanência da alocação dos equipamentos, *softwares* e demais elementos utilizados para a prestação dos serviços, que tenham sido instalados nas dependências do TCU, pelo período de 6 (seis) meses após o fim da vigência contratual, por meio da celebração de termo de cessão em comodato;

10.1. todas as funcionalidades providas pelos equipamentos, *softwares* e demais elementos devem continuar ativas, sem interrupções dos serviços por eles providos, inclusive suas consoles de gerência e configuração, com exceção de:

10.1.1. atualização das bases de dados, incluindo de antivírus/*antimalware* e de reputação;

10.1.2. assinaturas de atualização de equipamentos;

10.1.3. atualização de versão de *software*;

10.1.4. prestação dos serviços de “Monitoração e Administração de Segurança” e “Consolidação e Correlacionamento de Eventos”;

10.1.5. serviços gerenciados de segurança;

10.1.6. requisitos que exijam execução de atividades por parte de funcionários da contratada.

10.2. nesse período, não será exigida prestação dos serviços de suporte, manutenção e atualização dos produtos, nem garantia do fabricante.

11. os requisitos a seguir deverão ser atendidos por qualquer um dos itens contratadas:

    11.1. técnicas de detecção de programas de compartilhamento de arquivos (*peer-to-peer*) e de mensagens instantâneas, bloqueando aplicações como *Yahoo*! *Messenger*, *MSN Messenger*, *ICQ*, *AOL Messenger*, *BitTorrent*, *eDonkey*, *GNUTella*, *KaZaa*, *Skype* e *WinNY,* com pelo menos as seguintes funcionalidades:

        11.1.1. identificação do nome do usuário do programa de mensagens instantâneas;

        11.1.2. controle de:

            11.1.2.1. transferência de arquivos;

            11.1.2.2. conversas via áudio;

            11.1.2.3. transferência de fotos;

            11.1.2.4. sessões criptografadas.

    11.2. técnicas para proteção contra ataques do tipo *DDoS (Distributed Denial of Service)* e *DOS (Denial of Service),* sendo capaz de limitar ataques por:

        11.2.1. número de conexões *TCP* simultâneas por *IP* de origem, sem necessidade de especificar o endereço;

        11.2.2. conexões incompletas simultâneas por *IP* de origem, sem necessidade de especificar o endereço;

    11.3. a proteção deve abranger todos os usuários e serviços de rede do TCU, independente de sua localização física (*Datacenter* central, *Datacenter* de contingência, ISC ou nas Secretarias do TCU nos Estados);

12. o acesso à administração e ao monitoramento dos ativos deverá ser realizado somente a partir da rede TCU ou das instalações dos *SOCs* e dos *datacenters* da contratada e ser realizado por meio ou protocolo seguro, com registro de acesso detalhado;

13. os chamados deverão ser abertos por meio de central de atendimento localizada no Brasil, a partir de numero de ligação gratuita (0800) ou número local em Brasília, 24 horas por dia, 7 dias por semana, e por meio de portal na *Internet*;

14. o atendimento deve ser efetuado em língua portuguesa;

15. as atividades, quando realizadas no ambiente de produção, poderão ser agendadas para serem executadas após o expediente (horários noturnos, após as 20 horas, ou em finais de semana e feriados);

16. no momento de abertura do chamado, deverá ser fornecido ao TCU um número único de identificação e deverão ser classificados conforme a Tabela 8 – Atividades Operacionais de Segurança, contida no tópico IV – Nível Mínimo de Serviços. A classificação do chamado está sujeita a alteração pelo TCU sempre que este julgar necessário. Neste caso, os tempos de atendimento e resolução (NMS) serão contados a partir do momento em que o TCU efetue a solicitação de alteração de prioridade;

17. todos os chamados, bem como as providências adotadas, deverão ser armazenados em sistema para controle de chamados da contratada;

18. o acesso a esse sistema deverá estar disponível ao Tribunal e:

    18.1. devem ser criadas contas de usuários para que a equipe de servidores designados pelo TCU efetue o acesso ao sistema, para fins de auditoria e acompanhamento de andamento de chamdos;

    18.2. deve ser possível a extração de relatórios compreendendo o período integral do contrato;

19. os chamados abertos somente poderão ser fechados após autorização do TCU;

20. a contratada deverá realizar os devidos escalonamentos de acordo com a criticidade e nível de atendimento do incidente ou problema reportado pelo cliente ou pelo sistema de monitoração;

21. após resolução de um chamado técnico, a empresa contratada deverá encaminhar ao TCU relatório contendo descrição do chamado aberto, procedimento de resolução adotado e outros adicionais que poderão ser executados para que o problema ocorrido não se repita;

22. a contratada deverá realizar reuniões mensais, nas dependências do TCU;

23. a elaboração da ata de cada reunião será de responsabilidade da contratada, devendo ser enviada em até 5 (cinco) dias úteis após a realização da reunião;

24. as atividades a serem desenvolvidas nas reuniões mensais incluirão, entre outras:

    24.1. discussão e aprovação dos relatórios de fechamento mensais. O TCU terá o prazo de 5 (cinco) dias para efetuar a aprovação dos relatórios apresentados de acordo com os critérios estabelecidos neste Anexo;

    24.2. análise, discussão, entendimento e recebimento dos relatórios gerenciais e administrativos;

    24.3. apresentação do resumo de todos os registros feitos no sistema de abertura de chamados e do tratamento dado;

    24.4. revisão das configurações;

    24.5. procedimentos implementados.

25. a contratada deverá fornecer informações *on-line* do estado geral de segurança da rede (*dashboard*), contendo, no mínimo, o resumo quantitativo das seguintes informações:

    25.1. novas vulnerabilidades emergentes na internet;

    25.2. incidentes encontrados na rede TCU por *status* (encontrados, resolvidos e em tratamento);

    25.3. vulnerabilidades encontradas no TCU por status;

    25.4. volume e-mail/spam;

    25.5. disponibilidade dos serviços.

26. a contratada deverá fornecer mensalmente, em meio magnético ou eletrônico, os relatórios abaixo descritos:

26.1. dados, informações, indicadores e métricas que permitam quantificar a quantidade de solicitações para cada tipo de chamado, incluindo os chamados abertos pela contratada, com a média diária, semanal, mensal e anual;

26.2. dados, informações, indicadores e métricas que permitam quantificar o percentual de disponibilidade da central de atendimento da contratada, detalhados para a central de atendimento telefônico e para o portal na *Internet*;

26.3. atividades de suporte e manutenção, com pelo menos descrição de: problemas, correções, aplicações de *patches*, mudanças de configuração e eventos ocorridos no período;

26.4. inventário lógico de ativos de segurança;

26.5. controle de troca de equipamentos, com dados históricos de toda a duração do contrato;

26.6. chamados abertos no período, ações corretivas tomadas, tempos para execução das atividades;

26.7. diagnóstico dos ambientes monitorados, obtido por meio do cruzamento das informações obtidas nos *logs* coletados;

26.8. relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a qualidade e desempenho dos serviços prestados em relação ao atingimento ou não dos níveis mínimos de serviço, com, pelo menos, as seguintes informações:

26.8.1. NMS exigido, por item;

26.8.2. NMS alcançado, por item;

26.8.3. cálculo dos índices PD e FAIS (conforme tópico VIII deste Termo) de todos os itens;

26.8.4. cálculo do índice FADS (conforme tópico VIII deste Termo) de todas as atividades;

26.8.5. demonstrativos e relatórios que comprovem os cálculos efetuados;

26.8.6. razões e justificativas de toda violação identificada;

26.9. relatórios analíticos contendo dados, informações, indicadores e métricas gerenciais que permitam avaliar a qualidade e o desempenho dos serviços prestados com, pelo menos, as seguintes informações:

26.9.1. utilização de *CPU* e memória de todos os itens;

26.9.2. utilização de recursos diversos (discos, *cache*, rede etc);

26.9.3. disponibilidade de cada item;

26.9.4. atualizações de *software* realizadas no período;

26.9.5. total de chamados cadastrados por item;

26.9.6. classificação do chamado pelas prioridades estabelecidas;

26.9.7. tempo de atendimento por cada chamado aberto;

26.9.8. resumo do atendimento aos níveis mínimos de serviço;

26.10. relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a utilização dos serviços e recursos de rede com, pelo menos, as seguintes informações:

26.10.1. utilização de cada item em *Mbps*;

26.10.2. utilização de largura de banda das interfaces de rede;

26.10.3. sites com maior volume de dados acessados por esses usuários;

26.10.4. sites acessados por determinados usuários, classificado por username;

26.10.5. estatísticas de acesso *HTTP* e *HTTPS* por sub-rede IP em volume de dados (*MB*).

26.11. relatórios analíticos contendo dados, informações, indicadores e métricas que permitam identificar vulnerabilidades e sua exploração com, pelo menos, as seguintes informações:

26.11.1. ataques e tentativas de ataques à rede TCU;

26.11.2. análise e mitigação de ameaças (quantidade, estudo, mitigação, priorização);

26.11.3. análise de vulnerabilidades (quantidade, estudo, mitigação, priorização);

26.11.4. plano de ações sobre vulnerabilidades identificadas;

26.11.5. ameaças identificadas, segmentado item de serviço;

26.11.6. ações realizadas após ataques.

26.12. *baseline* (repositório) de pelo menos 1 (um) ano dos dados, informações, indicadores e métricas elaborados;

26.13. comprovação de que todos os *softwares* comerciais estão cobertos por contratos de suporte e atualização de versão e que todos os *hardwares* alocados estão cobertos por garantia do fabricante.

27. os dados referentes aos relatórios entregues deverão ser acessíveis em portal próprio, fornecido pela contratada, relativos aos últimos 90 (noventa) dias;

28. para realização da operação assistida, instalação, administração, aplicação de *patches* e mudanças de configuração dos equipamentos e *softwares* necessários à execução dos serviços e que exijam presença de técnico no local de instalação, e para realização das atividades do item 12 – Serviços Técnicos Especializados, a contratada deverá alocar profissionais que possuam as qualificações abaixo:

28.1. certificação no produto ou

28.2. experiência comprovada de 5 (cinco) anos na tecnologia.

29. para o planejamento e o acompanhamento da instalação dos equipamentos e *softwares* necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do *as-built*, e para demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens, a contratada deverá alocar profissionais que possuam qualificação *Project Management Professional* (*PMP*) ou *CompTIA Project+*;

30. para realização das reuniões mensais, deve alocar para atendê-las um gerente de serviços com perfil profissional que possua as qualificações abaixo:

    30.1. conhecer gerencialmente todos os serviços prestados da solução adotada;

    30.2. certificação em tecnologias de firewall ou de *IPS*.

31. para prestação dos serviços que exijam interação com o Comitê de Mudanças (*CAB*) do TCU e para o acompanhamento dos chamados e incidentes registrados, a contratada deverá alocar profissionais que possuam as qualificações abaixo:

    31.1. conhecimento de todos os serviços prestados da solução adotada;

    31.2. certificação em tecnologias de *firewall* ou de *IPS*.

32. para prestação dos serviços discriminadas no item 10 - Serviços de Monitoração e Administração de Segurança, deverão ser alocados profissionais que possuam as qualificações abaixo:

    32.1. certificação em tecnologias de *firewall,* de *IPS* e;

    32.2. experiência comprovada de 5 (cinco) anos nas tecnologias monitoradas.

33. as comprovações das qualificações definidas nos itens 27 a 31 devem ser feitas nos seguintes prazos:

    33.1. para operação assistida: na data de seu início;

    33.2. para instalação, administração, aplicação de *patches* e mudanças de configuração dos equipamentos e *softwares* necessários à execução dos serviços e que exijam presença de técnico no local de instalação: mensalmente, nas reuniões periódicas, mediante apresentação da lista de profissionais habilitados a realizá-las;

    33.3. para realização das atividades do item 12 – Serviços Técnicos Especializados: no momento da assinatura da ordem de serviço;

    33.4. para o planejamento e acompanhamento da instalação dos equipamentos e *softwares* necessários à execução dos serviços, da entrega das etapas para recebimento definitivo, da confecção do Projeto Executivo, da confecção do *as-built*, e para demais atividades pertinentes até a emissão do termo de recebimento definitivo de todos os itens: mensalmente, nas reuniões periódicas, mediante apresentação da lista de profissionais habilitados a realizá-las;

    33.5. para realização das reuniões mensais: no início de cada reunião;

33.6. para prestação dos serviços que exijam interação com o Comitê de Mudanças (*CAB*) do TCU e para o acompanhamento dos chamados e incidentes registrados: no início da reunião do *CAB* cuja presença técnica tenha sido solicitada;

33.7. para prestação dos serviços discriminadas no item 10 - Serviços de Monitoração e Administração de Segurança: mensalmente, nas reuniões periódicas, mediante apresentação da lista de profissionais habilitados a realizá-las.

34. as atividades listadas a seguir deverão ser realizadas durante toda a execução do contrato com alocação de profissional com qualificação técnica devidamente comprovada, de acordo com os requisitos definidos nos itens 27 a 31:

34.1. interação com o Comitê de Mudanças do TCU (*CAB*) sempre que solicitado, sendo possível a solicitação da participação física ou via telefone do técnico;

34.2. definição e implantação das rotinas de *backup* de todos os equipamentos componentes dos serviços. Nesse sentido, será responsabilidade da contratada o *backup* realizado pela própria, bem como a execução das configurações necessárias para realização de um *backup* secundário pelo *software* em uso atualmente pelo TCU (*IBM TSM*). No caso em que não seja possível efetuar o *backup* diretamente na solução, deverá ser provido um ponto único de coleta das configurações em formato texto para o *TSM*;

34.3. definição e validação dos procedimentos de recuperação para os equipamentos, produtos, peças ou *softwares* componentes da solução;

34.4. definição e implementação dos mecanismos permanentes de monitoramento dos equipamentos componentes da solução, inclusive com envio de informações de monitoramento para a solução em uso pelo Centro de Operação de Redes do TCU (*software Zabbix*);

34.5. configuração do *software* de monitoramento de rede do Tribunal (*software Zabbix*) para receber alarmes dos componentes da solução, conforme parâmetros a serem estabelecidos pelo Tribunal;

34.6. elaboração, atualização e manutenção da documentação "*as-built*", contendo:

34.6.1. características dos serviços;

34.6.2. topologias;

34.6.3. dados dos equipamentos, produtos, peças ou *softwares* utilizados no atendimento da solução, com respectivas configurações, números de série e demais informações pertinentes;

34.6.4. níveis mínimos de serviço;

34.6.5. atividades operacionais;

34.6.6. recorrências;

34.6.7. procedimentos para abertura e atendimento aos chamados;

34.6.8. definição de responsabilidades;

34.6.9. procedimentos para interrupções programadas;

34.6.10. *scripts* de operação (desligamento e religamento, *switch over*, acionamento do site de contingencia e instalação);

34.6.11. procedimentos de recuperação para os equipamentos componentes da solução;

34.6.12. procedimentos de replicação das configurações dos componentes da solução instalados no datacenter principal para componentes instalados no *datacenter* de contingência;

34.6.13. rotinas de *backup* e *restore* de todos os equipamentos, produtos, peças ou *softwares* componentes de cada um dos serviços.

34.7. fornecimento dos arquivos de configuração que possam ser acessíveis pela solução de *backup* e armazenamento do Tribunal;

34.8. execução de todas as atividades de transição dos serviços sob sua responsabilidade do *datacenter* central para o *datacenter* de contingência no TST, em casos de indisponibilidade do primeiro e do retorno dos serviços ao *datacenter* principal. Na ocasião, deverá verificar interdependências entre as aplicações, assegurando que as aplicações e serviços entrem em produção na sequência correta;

34.9. atualização do banco de dados de gerência de configuração (*CMDB* do *Service Desk*) para produtos, peças ou *softwares* necessários à prestação dos serviços;

34.10. elaboração, atualização e manutenção de toda a documentação descrita abaixo na base de conhecimentos do Tribunal (*MediaWiki*), incluindo:

34.10.1. procedimentos de recuperação para os equipamentos componentes da solução;

34.10.2. procedimento operacional para recuperação em caso de indisponibilidade do *datacenter* central (*disaster recovery)*;

34.10.3. controle de versões e procedimentos de *rollback*;

34.10.4. implementações e *scripts* padronizados para correção de problemas na configuração dos produtos, nas ferramentas e padrões especificados pelo Tribunal;

34.10.5. recursos de alta disponibilidade;

34.10.6. procedimentos e parâmetros para configuração, operação, instalação, manutenção, atualização e correto funcionamento dos componentes dos módulos de serviços;

34.10.7. modelos de configuração padrão (*templates*) e seus respectivos procedimentos de aplicação;

34.10.8. configurações implementadas;

34.10.9. rotinas de *backup* e *restore*;

34.10.10. *as-built*.

34.11. análise e implantação de ajustes nas permissões de acesso de usuários aos componentes da solução, mediante autorização prévia do Tribunal;

34.12. integração à base de usuários de rede do Tribunal (*Active Directory*) ou à plataforma de autenticação em uso pelo Tribunal (*Radius*) dos componentes da solução, nos casos previstos na especificação técnica;

34.13. mapeamento, junto ao TCU, de processos necessários ao cumprimento dos requisitos deste Termo;

34.14. comunicação ao Tribunal das providências adotadas em relação aos chamados, demandas e incidentes sob sua responsabilidade;

34.15. fornecimento, atualização e manutenção, a partir da assinatura do contrato, de relação dos técnicos indicados para atendimento local ao TCU, contendo:

34.15.1. nome;

34.15.2. RG;

34.15.3. resumo curricular;

34.15.4. comprovantes de certificação.

35. para todos os equipamentos, produtos ou peças utilizados na prestação dos serviços, a contratada deverá identificar, em local visível, por meio de etiqueta de material resistente, os equipamentos utilizados e os cabos de rede a eles conectados;

36. para todos os equipamentos, produtos ou *softwares* utilizados no atendimento aos requisitos destas Especificações Técnicas, deverão ser criadas:

36.1. conta de usuário com controle total para que a equipe de servidores designados pelo TCU de forma a possibilitar a atuação nos equipamentos em casos de indisponibilidade dos serviços da contratada, por quaisquer motivos;

36.2. contas de usuários para acesso pelos funcionários da contratada, mantidas em base de usuários local.

37. as contas de usuários com controle total referenciadas no item 33.1 somente serão utilizadas pelo TCU em momentos de indisponibilidade dos serviços da contratada, ou ainda, em situações de emergência em que a contratada viole os níveis mínimos de serviço contratada;

38. para todos os equipamentos, produtos ou *softwares* utilizados no atendimento aos requisitos deste Termo, deverão ser autorizados grupos de usuários (do *Active Directory* do Tribunal) para que a equipe do TCU possa monitorar e consultar informações nos equipamentos;

39. todos os equipamentos, produtos ou *softwares* necessários à prestação dos serviços deverão permitir consulta *on-line*, por meio de interface *WEB*, dos seus dados de saúde e desempenho;

40. quaisquer componentes adicionais que se fizerem necessários para que os produtos descritos ofereçam todas as características expostas, bem como para a perfeita instalação e utilização dos produtos, deverão ser providos pela contratada;

41. a equipe de servidores do TCU poderá, a qualquer momento, agendar vistorias nos ambientes de *SOC* e *datacenter* da contratada, de forma a averiguar o atendimento aos requisitos deste Termo;

42. no momento do envio da proposta comercial ajustada, o licitante deverá apresentar planilha de composição de custos detalhada de forma a permitir a repactuação futura do contrato;

IV. NÍVEL MÍNIMO DE SERVIÇOS (NMS)

A prestação dos serviços se baseará no modelo de remuneração em função dos resultados apresentados, em que os pagamentos serão feitos após mensuração e verificação de métricas quantitativas, contendo indicadores de desempenho e metas, com Nível Mínimo de Serviço (NMS) determinado em contrato, de modo a resguardar a eficiência e a qualidade na prestação dos serviços. Os níveis mínimos de serviço a seguir deverão ser registrados, monitorados e comparados às metas de desempenho e qualidade estabelecidas, em termos de prazo e efetividade, condição fundamental para efetuar a remuneração devida.

Os Níveis Mínimos de Serviço (NMS) serão divididos em Metas de Disponibilidade por Serviço e Atividades Operacionais de Segurança, além de indicadores próprios devidamente especificados, que deverão ser observados conforme as condições descritas neste item. Por conseguinte, o modelo de pagamento adotado no contrato será um modelo híbrido, de pagamento de serviço por disponibilidade, condicionada ao alcance de metas de desempenho. Dessa forma, os valores apresentados na proposta comercial do licitante correspondem aos valores máximos a serem faturados, na hipótese de a contratada atingir todos os níveis de serviço especificados.

As Metas de Disponibilidade Mensal deverão atender às seguintes condições:

1. para cada item de serviço (de 1 a 10), a Meta de Disponibilidade Mensal, deverá ser de, no mínimo:

Tabela 6 – Meta de Disponibilidade Mensal por Serviço

Item	Descrição	Meta de Disponibilidade Mensal (%)
1	Serviços de *Firewall* Central Externo	99,5
2	Serviços de *Firewall* e *VPN* Central Interno	99,5
3	Serviços de *Firewall* e *VPN* Remoto	96,5
4	Serviços de Prevenção de Intrusão Central	99,5
5	Serviços de *Proxy/cache* com filtro de conteúdo *WEB*	99,5
6	Serviços de *SMTP Antispam*	99,5
7	Serviços de *Firewall* de Aplicação	99,5

8	Serviços de Consolidação e Correlacionamento de Eventos	99,5
9	Serviços de Gestão de Vulnerabilidades	99,5
10	Serviços de Monitoração e Administração de Segurança	99,5

2. em cada período avaliado, o cálculo do Percentual de Disponibilidade (PD) para cada item de serviço se dará por meio da seguinte fórmula:

$$PD = \frac{[Tm - Ti]}{Tm} * 100, onde$$

PD é o Percentual de Disponibilidade Mensal;

Tm é o tempo total mensal de operação, em minutos, no mês de faturamento;

Ti é o somatório dos períodos de indisponibilidade dos serviços, em minutos, no mês de faturamento.

3. os Percentuais de Disponibilidade Mensal (PD) para o item 5 – Serviços de *Firewall* e *VPN* Remoto, referentes aos serviços que serão prestados nas Secretarias de Controle Externos nos Estados e no Instituto Serzedello Correa deverão ser calculados separadamente por localidade;

4. será computado como tempo de indisponibilidade (Ti):

4.1. o tempo em que o respectivo serviço esteja indisponível ou com desempenho degradado;

4.2. o tempo decorrido entre o início da indisponibilidade do serviço e sua total recuperação;

4.3. o tempo decorrido entre ocorrências sucessivas de indisponibilidade dentro de um intervalo inferior a 24 (vinte e quatro) horas do surgimento da primeira. Tais períodos serão considerados de "recorrência" da primeira ocorrência de indisponibilidade. Nesse caso, o tempo de indisponibilidade deverá ser contado a partir do surgimento da indisponibilidade inicial, até a recuperação da última indisponibilidade no intervalo;

4.4. o tempo decorrente de eventos sob responsabilidade da contratada, como queima de fontes de alimentação, mesmo que causada por queda ou variação de energia no ambiente do TCU, devendo a contratada, caso esta julgue pertinente, providenciar a devida proteção nos equipamentos instalados nas dependências do TCU;

4.5. o tempo decorrente de impossibilidade de acesso dos técnicos da contratada ao ambiente do TCU para resolução de problemas. Nesse caso, sempre que ocorrer a necessidade comprovada de verificação no ambiente do TCU, a contratada deverá contatar o responsável pelo local de instalação e, caso não seja possível, deverá contatar o centro de operações de rede do TCU. Somente será admitida a interrupção da contagem dos tempos de indisponibilidade em

caso de evento que ocorra fora dos horários cobertos pelo centro de operações de rede do TCU.

5. não serão incluídas na contagem do número de minutos de indisponibilidade (Ti) as seguintes situações que ocorram nas instalações do TCU:

   5.1. falta de energia no local;

   5.2. indisponibilidade da rede lógica do TCU à qual o item esteja conectado;

   5.3. manutenções programadas pelo TCU e manutenções programadas pela contratada, desde que autorizadas previamente pelo TCU;

   5.4. problemas derivados de ocorrências no ambiente do TCU, onde comprovadamente a indisponibilidade não esteja sendo controlada pela contratada;

   5.5. ações necessárias para resolução de problemas que não tenham sido autorizadas pelo TCU.

6. durante a prestação dos serviços, deverá ser computado, ainda, o Número de Ocorrências de Indisponibilidade (NOI). O valor NOI deverá ser calculado para cada item de serviço e servirá de base para mensuração da qualidade dos serviços;

7. chamados abertos cujo prazo de resolução encerre somente no próximo período de faturamento somente terão calculados os fatores de abatimento a partir período seguinte;

8. a disponibilidade para o item 10 - Serviços de Monitoração e Administração de Segurança será medida pelos seguintes eventos:

   8.1. indisponibilidade da central de atendimento telefônico;

   8.2. indisponibilidade do portal de serviços na *Internet*;

9. os Fatores de Abatimento por Indisponibilidade de Serviços (FAIS) relativos ao Percentual de Disponibilidade Mensal deverão, ainda, ser multiplicados por um Fator de Peso do Item (FPI), segundo a Tabela 7 a seguir, por tipo de serviço:

Tabela 7 – Fator de Peso do Item - FPI

Item	Descrição do itens	Fator de Peso do Item (FPI)
1	Serviços de *Firewall* Central Externo	2,0
2	Serviços de *Firewall* e *VPN* Central Interno	2,0
3	Serviços de *Firewall* e *VPN* Remoto	1,5
4	Serviços de Prevenção de Intrusão Central	1,5
5	Serviços de *Proxy/cache* com filtro de conteúdo *WEB*	1,5
6	Serviços de *SMTP Antispam*	1,5

7	Serviços de *Firewall* de Aplicação	2,0
8	Serviços de Consolidação e Correlacionamento de Eventos	2,0
9	Serviços de Gestão de Vulnerabilidades	1,0
10	Serviços de Monitoração e Administração de Segurança	2,0

10. dessa forma, o Fator de Abatimento por Indisponibilidade de Serviço (FAIS) no valor das faturas mensais será calculado, por item, de acordo com a seguinte fórmula:

$$FAIS = \sum_{k=1}^{10} VMI_k \times FPI_k \times \left\{ \left[\frac{(MDM_K - Min(MDM_K, PD_K))}{100} \times MTI \right] + \left[\frac{Max(NOI_K, 1) - 1}{100} \right] \right\}$$

k é o número do item de serviço;

FAIS é o Fator de Abatimento por Indisponibilidade de Serviço;

VMI é o valor mensal do item;

MDM é a meta de disponibilidade mensal do item;

PD é o Percentual de Disponibilidade Mensal, calculado segundo a fórmula supracitada;

MTI é o multiplicador por tempo de indisponibilidade,conforme definido a seguir:

1 – se (MDM – PD) menor ou igual 1;

2 – se (MDM – PD) maior que 1 e menor ou igual a 5;

3 – se (MDM – PD) for maior que 5;

FPI é o Fator de Peso do Item;

NOI é o número de ocorrências de indisponibilidade do item no mês;

Max é a função que retorna o valor máximo;

Min é a função que retorna o valor mínimo.

Além da Meta de Disponibilidade Mensal, deverão ser apurados os níveis de serviço para as Atividades Operacionais de Segurança a seguir, que deverão ser executadas periodicamente pela contratada ou por demanda pelo TCU:

1. para os itens de serviço de 1 a 10, em conjunto, serão estabelecidos os seguintes prazos máximos de conclusão das atividades, os indicadores utilizados na mensuração da qualidade dos serviços e os respectivos fatores de abatimento pelo descumprimento dos níveis mínimos de serviço associados:

Tabela 8 – Atividades Operacionais de Segurança

Atividade	Nível Mínimo de Serviço (NMS)	IndMeta	Indicador para NMS	Fator de Peso da Atividade (FPA)
1 - Gerenciamento de regras e políticas	120 minutos após abertura de chamado	120 min	Regra implementada	0,5
2- Alteração de configurações	240 minutos após abertura de chamado	240 min	Configuração implementada	0,5
3 - Chamados Emergenciais (limitados a 20 por mês e relacionados apenas a gerenciamento de regras ou alteração de configurações)	20 minutos após abertura de chamado	20 min	Chamado concluído	1
4 - Verificação e filtragem de *logs*	24 horas após abertura de chamado	24 h	Arquivo de *log* enviado ao solicitante	0,25
5 - Atualização de plataformas por meio da implementação de *patches* e *fixes*	5 dias após liberação das atualizações pelo fabricante, incluído neste limite o tempo necessário à homologação do pacote pela contratada	5 d	*Patch* e *fix* instalados	0,5
6 - Registro de incidentes de segurança pela contratada	10 minutos após o primeiro registro ou sintoma relacionado ao evento	10 min	Chamado aberto	0,1
7 - Início de atuação para resolução de incidentes de segurança	15 minutos após abertura de chamado pelo cliente ou pela contratada	15 min	Registro das ações tomadas no chamado pelo responsável pela resolução	0,5
8 - Resolução de incidentes que provoquem indisponibilidade dos serviços e que não necessitem substituição de peças	60 minutos após abertura de chamado pelo cliente ou pela contratada	60 min	Chamado concluído	1,5
9 - Resolução de incidentes que não provoquem indisponibilidade dos serviços	240 minutos após abertura de chamado pelo cliente ou pela contratada	240 min	Chamado concluído	0,5

10 - Atendimento a chamados para esclarecimento de dúvidas	72 horas após abertura de chamado pelo cliente	72 h	Chamado concluído	0,1
11 - Implementação de novas funcionalidades	72 horas após abertura de chamado pelo cliente ou pela contratada	72 h	Funcionalidade implementada	0,5
12 - Geração de assinaturas de reconhecimento de ataques	360 minutos após abertura de chamado pelo cliente ou pela contratada	360 min	Assinatura de ataque implementada	0,1
13 - Atualização de bases externas de categorização de *sites*, mensagens, vírus, *malware*, assinatura de ataques e vulnerabilidades	12 horas após liberação pelo fabricante	12 h	Base de assinaturas atualizada	0,5
14 - Criação e implantação de conectores para consolidação e correlacionamento de Eventos	72 horas após abertura de chamado	72 h	Conector implementado	0,1
15 - Realização periódica de *scan* de vulnerabilidades em ativos de criticidade alta	Semanal, apresentado toda segunda-feira	7 d	Relatório de vulnerabilidades apresentado	0,5
16 - Realização periódica e *scan* de vulnerabilidades em ativos de criticidade baixa	Mensal, apresentado na primeira segunda-feira do mês	30 d	Relatório de vulnerabilidades apresentado	0,1
17 - Realização de *scan* sob demanda	24 horas após abertura de chamado pelo cliente	24 h	Relatório de vulnerabilidades apresentado	0,1

2. os Fatores de Abatimento por Desempenho de Serviço (FADS) serão calculados com base na comparação dos resultados alcançados na execução das atividades com os níveis de serviço definidos na Tabela 8 – Atividades Operacionais de Segurança.
3. o FADS será calculado como somatório das ocorrências realizadas para cada uma das atividades definidas, conforme fórmula a seguir:

$$FADS = \sum_{i=1}^{17} \sum_{j=1}^{n} VMC \times \left[\frac{Max(IndAting_{i,j}, IndMeta_i) - IndMeta_i}{10 \times IndMeta_i} \right] \times FPA_i$$

i é o número da atividade;

j é o contador de ocorrências da atividade que não atenderam o NMS definido;

n é a quantidade de ocorrências da atividade que não atenderam o NMS definido;

FADS é o Fator de Abatimento por Desempenho de Serviço;

VMC é o valor mensal do contrato;

IndMeta – é o índice de meta (NMS), em minutos/horas/dias, definido para a atividade;

IndAting – é o índice atingido, em minutos/horas/dias, pela atividade que ultrapassou o NMS;

FPA é o Fator de Peso da Atividade;

Max é a função que retorna o valor máximo.

Para o item 11 (Treinamento), deverão ser calculados os Fatores de Abatimento por Entrega de Treinamento (FATR), de acordo com a fórmula abaixo:

$$FATR = VTR \times Min\left(1 \ , \ \left[\frac{NUM\,\mathrm{Re}marc}{10} + \frac{(NUM\,\mathrm{Re}v - 1)}{20} + \frac{NUM\,\mathrm{Re}pet}{5}\right]\right)$$

VTR é valor da Ordem de Serviço de Treinamento, em reais;

NUMRemarc é o número de vezes que o treinamento foi remarcado devido a problemas com o material didático ou de responsabilidade da contratada;

NUMRev é o número de vezes que o material didático foi submetido pela contratada à revisão pelo TCU;

NumRepet é o número de vezes que o treinamento foi repetido devido a ter sido considerado insatisfatório.

Por fim, para o item 12 (Serviços Técnicos Especializados), também deverão ser calculados os Fatores de Abatimento por Entrega de Produto (FAEP), de acordo com a fórmula abaixo:

$$FAEP = VOS \times Min\left(1 \ , \ \left[\frac{NDUAtraso}{MDOS \times NDUOS} + \frac{(NUM\,\mathrm{Re}v - 1)}{20}\right]\right)$$

VOS é valor da Ordem de Serviço, em reais;

NDUAtraso é o número de dias úteis de atraso;

NDUOS é o número de dias úteis do prazo de execução definido na Ordem de Serviço;

NUMRev é o número de vezes que os produtos da respectiva ordem de serviço foram submetidos à revisão pelo TCU;

MDOS é o multiplicador de duração da Ordem de Serviço, variando de acordo com o número de dias úteis do prazo de execução definido na Ordem de Serviço, conforme tabela a seguir:

Prazo de execução	MDOS
Até 10 dias úteis	4
Acima de 10 dias úteis	2

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

Os serviços de que tratam os itens 1 a 10 referem-se à prestação de serviços mensais, de natureza contínua, razão pela qual podem vigorar pelo período de até 60 meses, tendo como fundamento o que dispõe o inc. II, art. 57 da Lei nº 8.666/93. O período de prestação, a partir da emissão do termo de recebimento definitivo, será o estabelecido na tabela abaixo, observadas as etapas previstas no item XIV – Planejamento, customização de ambiente e instalação de ativos de rede, deste Termo.

Tabela 11 – Período de Prestação dos Serviços

Item	Descrição	Quantidade	Meses
1	Serviços de *Firewall* Central Externo	1	60
2	Serviços de *Firewall* e *VPN* Central Interno	1	60
3	Serviços de *Firewall* e *VPN* Remoto	29	56
4	Serviços de Prevenção de Intrusão Central	2	53
5	Serviços de *Proxy*/*cache* com filtro de conteúdo *WEB*	1	57
6	Serviços de *SMTP Antispam*	1	57
7	Serviços de *Firewall* de Aplicação	1	53
8	Serviços de Consolidação e Correlacionamento de Eventos	1	60
9	Serviços de Gestão de Vulnerabilidades	1	56
10	Serviços de Monitoração e Administração de Segurança	1	60

O item 11 refere-se à prestação de serviços de treinamento que deverão ser solicitados por meio de Ordem de Serviço de Treinamento (Anexo VIII) cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços de Treinamento (Anexo VII). Tais serviços deverão ser prestados em, no máximo, 4 (quatro) meses após o recebimento definitivo dos serviços alvo do treinamento.

O item 12 refere-se à prestação de serviços técnicos especializados de natureza eventual, sendo demandados de acordo com as necessidades do Tribunal, solicitados por meio de Ordem de Serviço (Anexo VIII) cuja execução deve ser recebida por meio do Termo de Recebimento de Serviços (Anexo VII).

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

1. reunião de início do projeto (*kick-off*): 10 (dez) dias corridos;
2. entrega do Projeto Executivo: 40 (quarenta) dias corridos;
   2.1. o TCU se manifestará no prazo de 10 (dez) dias corridos, contados da data de entrega do Projeto Executivo;
   2.2. havendo necessidade de ajustes, a contratada terá 10 (dez) dias corridos para realizá-los, contados da notificação a ser efetuada pelo Tribunal, a respeito da manifestação sobre o Projeto Executivo;

3. início da planejamento, customização e instalação de elementos da etapa I: 60 (sessenta) dias corridos;
4. os prazos para término do planejamento, customização e instalação dos elementos de cada etapa devem ser de, no máximo:
   4.1. etapa I: início em 60 dias e término em até 150 dias;
   4.2. etapa II: início com 150 dias e término em até 180 dias;
   4.3. etapa III: início com 180 dias e término em até 270 dias;
   4.4. etapa IV: início com 270 dias e término em até 360 dias;
5. a contratada poderá concluir o planejamento, a customização e a instalação de uma etapa antes do fim do prazo estipulado, porém não poderá iniciar a instalação da etapa seguinte em data anterior à prevista sem a expressa anuência do titular da ***Diretoria de Gestão do Ambiente Computacional – Diamb/Setic***;
6. o termo de recebimento definitivo de cada item (de 1 a 10) obedecerá aos seguintes critérios:
   6.1. o TCU terá 15 (quinze) dias corridos para emitir o termo de recebimento definitivo, depois de finalizado o planejamento, a customização e a instalação de cada item;
   6.2. a prestação dos serviços e a respectiva remuneração, com o respectivo início de faturamento, iniciarão apenas após a emissão do termo de recebimento definitivo;
   6.3. para todos os bens importados que forem instalados nas dependências do TCU será necessária a apresentação dos respectivos comprovantes de origem.
7. os SOCs e os datacenters da contratada deverão estar em pleno funcionamento, operando em regime 24x7x365, em até 60 dias contados da assinatura do contrato.

VI. PAGAMENTO

O pagamento dos itens 1 a 10 será feito mensalmente, levando-se em consideração o Nível Mínimo de Serviço (NMS) acordado em contrato, para o período de faturamento avaliado.

De forma a viabilizar a análise da prestação dos serviços, a contratada deverá apresentar, na forma de relatório, informações acerca da aferição dos níveis de serviço contratadas. Deverão ser detalhados todos os tempos de atendimento a todas as ocorrências assim como o cálculo do Percentual de Disponibilidade Mensal (PD) para verificação de atingimento de metas, conforme a Tabela 6 do tópico IV – Nível Mínimo de Serviços. Além disso, os relatórios devem apresentar a descrição de todas as atividades realizadas no período, elencadas conforme a Tabela 8, do mesmo tópico, e o cálculo detalhado dos diversos fatores de abatimento previstos no Termo de Referência (FAIS, FADS, FATR, FAEP).

A reunião mensal deverá ocorrer até o 5º (quinto) dia útil após o término do período de faturamento, que coincidirá com o mês legal, e a entrega dos relatórios será condição

necessária ao recebimento dos serviços pelo TCU. O primeiro mês de faturamento será parcial, contado da data da emissão do termo de recebimento definitivo do item até o último dia do mês.

A respectiva nota fiscal/fatura, já deduzidos os fatores de abatimento calculados, deverá ser emitida somente após o recebimento definitivo dos serviços e após a homologação das informações apresentadas pela contratada ao TCU.

Caso não haja concordância, por parte da contratada, em relação aos fatores de abatimento calculados, os mesmos serão convertidos em sanção, com aplicação de multa de mesmo valor, de forma a garantir o contraditório e a ampla defesa.

Já o pagamento do item 11 será feito após a ordem de serviço de treinamento (conforme modelo aposto ao Anexo VI) ser emitida e os serviços prestados de maneira satisfatória (conforme modelo de Termo de Recebimento de Serviços de Treinamento aposto ao Anexo VII), respeitados os prazos definidos no item 11 (Treinamento). A nota fiscal/fatura relativa à prestação dos serviços, já considerado o FATR, deverá ser emitida somente após o recebimento dos serviços pelo TCU.

E, finalmente, o pagamento do item 12 será feito após a ordem de serviço (conforme modelo aposto ao Anexo VIII) ser emitida e os serviços prestados de maneira satisfatória (conforme modelo de Termo de Recebimento de Serviços aposto ao Anexo VII), respeitados os prazos definidos no item 12 (Serviços Técnicos Especializados). A nota fiscal/fatura relativa à prestação dos serviços, já considerado o FAEP, deverá ser emitida somente após o recebimento dos serviços pelo TCU.

VII. SANÇÕES

A contratada ficará sujeita, nos casos de inadimplemento injustificado, assim considerado pela Administração, inexecução parcial ou inexecução total da obrigação, sem prejuízo das responsabilidades civil e criminal e demais sanções previstas na legislação, asseguradas a ampla defesa prévia e o contraditório, às seguintes penalidades:

1. 1% (um por cento) do valor total mensal do contrato, por ocorrência, pelo descumprimento ou inobservância a qualquer item estabelecido no tópico – Planejamento, Customização de Ambiente e Instalação de Ativos de Rede;
2. 1% (um por cento) do valor total mensal do contrato, por ocorrência, pelo descumprimento ou inobservância a qualquer item estabelecido nos Requisitos Gerais para Prestação dos Serviços;
3. 10% (dez por cento) do valor total mensal do contrato pelo descumprimento ou inobservância a qualquer item estabelecido no tópico – Transição Contratual, destas especificações técnicas;
4. 1% (hum por cento) do valor total mensal do contrato, por dia de atraso no prazo de atendimento a qualquer prazo estabelecido no tópico – Prazos de Execução e de Aceite e Natureza dos Serviços, destas especificações técnicas;
5. 3% (três por cento) do valor total mensal do contrato, por ocorrência, caso seja identificada nas bases de usuário mantidas pela contratada conta com acesso às

soluções implementadas, cujo detentor não mais faça parte da equipe que atue no contrato;

6. 30% (trinta por cento) do valor do treinamento, por ocorrência, caso o treinamento não seja realizado;
   a. será considerado como não realizado o treinamento que precise ser repetido mais de 2 vezes, por insuficiência;
7. 30% (trinta por cento) do valor da Ordem de Serviço, por ocorrência, caso produto definido em Ordem de Serviço, emitida e assinada pela contratada, não seja entregue;
   a. será considerado como não entregue, produto que atrase por período igual a 3 (três) vezes o período de execução definido na Ordem de Serviço;
8. 15% (quinze por cento) do valor total mensal do contrato, por ocorrência, pelo descumprimento ou inobservância a qualquer item estabelecido no Termo de Confidencialidade e Sigilo da Contratada – Anexo V do Edital do Pregão Eletrônico n.º 86/2011;
9. 5% (cinco por cento) do valor total mensal do contrato, por indicador ou meta de nível de serviço, que tenha sido objeto de tentativa de burla, fraude, manipulação ou descaracterização pela contratada;
10. 0,5% (cinco décimos por cento) do valor total mensal do contrato, por ocorrência, em caso de fechamento não autorizado de chamados;
11. 2% (dois por cento) do valor total mensal do contrato, por ocorrência que permaneça sem solução por mais de um período de faturamento consecutivo;
12. 15% (quinze por cento) do valor total mensal do contrato no caso de:
    a. incompatibilidade entre os serviços providos e a infraestrutura computacional do TCU;
    b. entrega de serviços fora das especificações técnicas exigidas;
    c. mais de um item de serviço de natureza continuada com valor zerado no mês em função de não cumprimento da Meta de Disponibilidade Mensal estabelecida;
    d. o mesmo item de serviço de natureza continuada com valores zerados em meses consecutivos em função de não cumprimento de Meta de Disponibilidade Mensal estabelecida.

VIII. LOCAL DE EXECUÇÃO DOS SERVIÇOS

Os serviços serão executados no Edifício Sede e Anexos do Tribunal de Contas da União (TCU) em Brasília, nas Secretarias de Controle Externo (Secex) em cada um dos Estados do país, no Instituto Serzedello Correa (ISC) em Brasília e no Tribunal Superior do Trabalho (TST),

conforme os endereços a seguir. Essas informações podem também ser verificadas, exceto aquelas relativas ao TST e à Sede - DF, no Portal do TCU na *Internet*:

http://portal2.tcu.gov.br/portal/page/portal/TCU/institucional/conheca_tcu/contatos,

Tribunal de Contas da União (TCU) – *Datacenter* principal
Endereço: SAFS - Quadra 04 - Lote 01
CEP: 70042-900 Brasília – DF

Tribunal Superior do Trabalho (TST) – *Datacenter* de contingência
Endereço: SAFS - Quadra 08, Lote 01
Brasília-DF

Instituto Serzedello Corrêa (ISC)
Endereço: SCS Quadra 09 Bloco A Torre B 6º Andar - Ed. Parque Cidade Corporate
CEP: 70308-200 Brasília - DF

Secretaria de Controle Externo do Acre (SECEX-AC)
Endereço: Rua Guiomard Santos, 353 – Bosque
CEP: 69909-370 Rio Branco – AC

Secretaria de Controle Externo de Alagoas (SECEX-AL)
Endereço: Av. Assis Chateaubriand, nº 4.118 - Trapiche da Barra
CEP: 57010-070 Maceió – AL

Secretaria de Controle Externo do Amapá (SECEX-AP)
Endereço: Rua Cândido Mendes, 501 – Centro
CEP: 68906-260 Macapá – AP

Secretaria de Controle Externo do Amazonas (SECEX-AM)
Endereço: Av. Joaquim Nabuco, 1193 – Centro
CEP: 69020-030 Manaus – AM

Secretaria de Controle Externo da Bahia (SECEX-BA)
Endereço: Av. Tancredo Neves, nº 2242 – STIEP
CEP: 41820-020 Salvador – BA

Secretaria de Controle Externo do Ceará (SECEX-CE)
Endereço: Av. Valmir Pontes, nº 900 - Bairro Edson Queiroz
CEP: 60812-020 Fortaleza – CE

Secretaria de Controle Externo do Distrito Federal (SECEX-DF)
Endereço: SAFS - Quadra 04 - Lote 01 – Anexo II – Sala 50
CEP: 70042-900 Brasília – DF

Secretaria de Controle Externo do Espírito Santo (SECEX-ES)
Endereço: Rua Luiz Gonzalez Alvarado, s/nº - Enseada do Suá
CEP: 29050-380 Vitória – ES

Secretaria de Controle Externo do Goiás (SECEX-GO)
Endereço: Av. Couto Magalhães, nº 277 - Setor Bela Vista
CEP: 74823-410 Goiânia – GO

Secretaria de Controle Externo do Maranhão (SECEX-MA)
Endereço: Av. Senador Vitorino Freire, nº 48 - Areinha - Trecho Itaqui/Bacanga
CEP: 65010-650 São Luís – MA

Secretaria de Controle Externo do Mato Grosso (SECEX-MT)
Endereço: Rua 2 - esquina com Rua C - Setor A - Quadra 4 - Lote 4 - Centro Político Administrativo (CPA)
CEP: 78050-970 Cuiabá – MT

Secretaria de Controle Externo do Mato Grosso do Sul (SECEX-MS)
Endereço: Rua da Paz, 780 - Bairro Jardim dos Estados
CEP: 79020-250 Campo Grande – MS

Secretaria de Controle Externo das Minas Gerais (SECEX-MG)
Endereço: Rua Campina Verde, 593 - Salgado Filho
CEP: 30550-340 Belo Horizonte – MG

Secretaria de Controle Externo do Pará (SECEX-PA)
Endereço: Travessa Humaitá, nº 1574
CEP: 66085-220 Belém – PA

Secretaria de Controle Externo da Paraíba (SECEX-PB)
Endereço: Praça Barão do Rio Branco, 33 – Centro
CEP: 58010-760 João Pessoa – PB

Secretaria de Controle Externo do Paraná (SECEX-PR)
Endereço: Rua Dr. Faivre nº 105 – Centro
CEP: 80060-140 Curitiba – PR

Secretaria de Controle Externo de Pernambuco (SECEX-PE)
Endereço: Rua Major Codeceira, nº 121 - Bairro Santo Amaro
CEP: 50100-070 Recife – PE

Secretaria de Controle Externo do Piauí (SECEX-PI)
Endereço: Av. Pedro Freitas, 1904 - Centro Administrativo
CEP: 64018-000 Teresina – PI

Secretaria de Controle Externo do Rio de Janeiro (SECEX-RJ)
Endereço: Rua Buenos Aires, 256 – 4º andar – Centro
CEP: 20061-000 Rio de Janeiro – RJ

9ª Secretaria de Controle Externo (SECEX-9)
Endereço: Av. Presidente Antonio Carlos, nº 375 - Edifício do Ministério da Fazenda - 12º andar Sala 1204
CEP: 20020-010 Rio de Janeiro – RJ

Secretaria de Controle Externo do Rio Grande do Norte (SECEX-RN)
Endereço: Av. Rui Barbosa, 909 - Morro Branco
CEP: 59075-300 Natal – RN

Secretaria de Controle Externo do Rio Grande do Sul (SECEX-RS)
Endereço: R. Caldas Júnior, nº 120 - 20º andar - Ed. Banrisul – Centro
CEP: 90018-900 Porto Alegre – RS

Secretaria de Controle Externo de Rondônia (SECEX-RO)
Endereço: Rua Afonso Pena, 345 – Centro
CEP: 76801-100 Porto Velho – RO

Secretaria de Controle Externo de Roraima (SECEX-RR)
Endereço: Av. Ville Roy, 5297 - Bairro São Pedro
CEP: 69306-665 Boa Vista – RR

Secretaria de Controle Externo de Santa Catariana (SECEX-SC)
Endereço: Rua São Francisco, 234 – Centro
CEP: 88015-140 Florianópolis – SC

Secretaria de Controle Externo de São Paulo (SECEX-SP)
Edifício Cetenco Plaza – Torre Norte - Avenida Paulista, 1842, 25º andar
CEP: 01310-923 - São Paulo – SP

Secretaria de Controle Externo de Sergipe (SECEX-SE)
Endereço: Av. Dr. Carlos Rodrigues da Cruz, 1340 - Centro Administrativo Augusto Franco – CENAF
CEP: 49080-903 Aracaju – SE

Secretaria de Controle Externo de Tocantins (SECEX-TO)
Endereço: 302 Norte - Av. Teotônio Segurado - Lote 1A - Plano Diretor Norte
CEP: 77001-020 Palmas - TO

IX. TRANSIÇÃO CONTRATUAL

A contratada deverá elaborar e entregar procedimentos de transição contratual para cada um dos itens de serviço. Tais documentos serão responsáveis por assegurar a

disponibilidade dos serviços de TI no momento de migração, como subsídio para contratações futuras, incluindo as seguintes informações e ações:

1. atualização da documentação, compreendendo *as-built*, parâmetros de instalação e configuração, arquitetura e topologias implementadas, entre outros;
2. *baselines* com dados que subsidiem o planejamento de capacidade para todos os itens de serviço com, pelo menos, informações estatísticas de utilização dos recursos dos equipamentos e *softwares* alocados (recursos de memória, de *CPU*, de rede, de *I/O* etc);
3. demonstrativo de crescimento anual, compreendendo toda a vigência do contrato, para todos os itens de serviço;
4. esclarecimento de dúvidas de configuração, dimensionamento ou operação;
5. fornecimento de arquivos de configuração dos produtos;
6. recolhimento dos equipamentos, produtos, peças ou *softwares* necessários à prestação dos serviço**s**, em seus locais de instalação ou em local a ser designado pelo TCU**.**

ANEXO III – MODELO DE PLANILHA DE PROPOSTA DE PREÇOS

O valor total da contratação está estimado em 15.859.636,12 (quinze milhões oitocentos e cinquenta e nove mil seiscentos e trinta e seis reais e doze centavos) para o período de 60 (sessenta) meses. Embora a adjudicação seja global, o **licitante** deverá enviar proposta com os valores discriminados por itens, conforme a seguir:

Item	Descrição	Meses	Quant	Valor mensal/unidade (R$)	Valor Total (R$)
1	Serviços de *Firewall* Central Externo	60	1		
2	Serviços de *Firewall* e *VPN* Central Interno	60	1		
3	Serviços de *Firewall* e *VPN* Remoto	56	29		
4	Serviços de Prevenção de Intrusão Central	53	2		
5	Serviços de *Proxy/cache* com filtro de conteúdo *WEB*	57	1		
6	Serviços de *SMTP Antispam*	57	1		
7	Serviços de *Firewall* de Aplicação	53	1		
8	Serviços de Consolidação e Correlacionamento de Eventos	60	1		
9	Serviços de Gestão de Vulnerabilidades	56	1		
10	Serviços de Monitoração e Administração de Segurança	60	1		
			Quant	**Valor unitário (R$)**	**Valor Total (R$)**
11	Treinamentos				

11.1	*Firewall* Central Externo		1		
11.2	*Firewall* e *VPN* Central Interno		1		
11.3	*Firewall* e *VPN* Remoto		1		
11.4	Prevenção de Intrusão Central		1		
11.5	*Proxy/cache* com filtro de conteúdo *WEB*		1		
11.6	*SMTP* (Antispam)		1		
11.7	*Firewall* de Aplicação		1		
11.8	Consolidação e Correlacionamento de Eventos		1		
11.9	Gestão de Vulnerabilidades		1		
11.10	Monitoração e Administração de Segurança		1		
12	Serviços Técnicos Especializados		1600		
TOTAL					

Observações:

a) Todos os **licitantes** deverão apresentar planilha de composição de custos detalhada anexa à proposta comercial;

b) Não deverão ser oferecidos preços com valores superiores aos expressos na coluna de valores máximos da tabela 10 abaixo. Caso o **licitante** assim proceda, deverá apresentar, ainda durante a fase de habilitação do pregão, justificativa detalhada, informando os motivos e os componentes de custo que levaram a oferta ao patamar referenciado.

c) Caso o **licitante** apresente valores inferiores aos expressos na coluna de valores de referência para exequibilidade, deve comprovar a viabilidade da execução contratual da proposta, ainda durante a fase de habilitação do pregão, por meio de demonstrativo analítico de todos os custos e receitas envolvidas.

Tabela 10 – Limites de Aceitabilidade de Preços e de Exequibilidade da Proposta

Item	Valor de referência para exequibilidade (R$)	Valor máximo (R$)
1	266.070,00	1.046.813,33
2	391.217,82	1.516.156,50
3	404.528,71	1.424.053,68
4	446.558,23	1.368.947,73
5	514.690,85	2.046.362,91
6	418.950,00	1.426.939,78
7	373.448,60	841.279,14
8	600.600,00	3.778.066,50
9	225.635,20	1.046.600,80
10	458.542,56	3.406.058,55
	Valor mínimo (R$)	Valor máximo (R$)
11.1	1.968,04	15.818,77
11.2	1.968,04	15.818,77
11.3	1.614,29	15.437,17
11.4	1.260,54	13.055,58
11.5	1.260,54	13.055,58
11.6	1.260,54	13.055,58
11.7	1.968,04	15.818,77

11.8	1.260,54	13.055,58
11.9	906,79	11.673,98
11.10	906,79	11.673,98
12	161.280,00	320.380,44
		Valor global máximo (R$)
		15.859.636,12

d) Devem ser informadas as marcas, modelos e quantidades de todos os equipamentos, produtos, peças ou *softwares* necessários à correta prestação dos serviços, assim como a descrição de como será feito o atendimento aos requisitos do Termo de Referência, incluindo-se a informação de ocupação de U's pela solução proposta pelo **licitante**.

ANEXO IV – TERMO DE CONFIDENCIALIDADE E SIGILO DO LICITANTE

A empresa [RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Tribunal de Contas da União – TCU, aceita as regras, condições e obrigações constantes do presente Termo.

1. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do TCU reveladas à EMPRESA RECEPTORA em função da vistoria prévia realizada para atendimento ao Edital do Pregão Eletrônico n.º 86/2011.

2. 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 idéias, outras informações técnicas, financeiras ou comerciais, entre outros.

3. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do TCU, das informações restritas reveladas.

4. 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 TCU, as informações restritas reveladas.

5. 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 TCU, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

6. 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.

7. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao TCU 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.

8. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do TCU, possibilitará a imediata rescisão de qualquer contrato firmado entre o TCU e a EMPRESA RECEPTORA sem qualquer ônus para o TCU. Nesse caso, a EMPRESA RECEPTORA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo TCU, inclusive os de ordem moral, bem como as responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

9. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do TCU.

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, ___ de _____ de 20__.

[NOME DA EMPRESA RECEPTORA]

_____
Nome:

_____
Nome:

ANEXO V – TERMO DE CONFIDENCIALIDADE E SIGILO DA CONTRATADA

A empresa [RAZÃO/DENOMINAÇÃO SOCIAL], pessoa jurídica com sede em [ENDEREÇO], inscrita no CNPJ/MF com o n.º [N.º DE INSCRIÇÃO NO CNPJ/MF], neste ato representada na forma de seus atos constitutivos, doravante denominada simplesmente EMPRESA RECEPTORA, por tomar conhecimento de informações sobre o ambiente computacional do Tribunal de Contas da União – TCU, aceita as regras, condições e obrigações constantes do presente Termo.

1. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do TCU reveladas à EMPRESA RECEPTORA em função da prestação dos serviços objeto do contrato n.º 86/2011.

2. 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.

3. A EMPRESA RECEPTORA compromete-se a não reproduzir nem dar conhecimento a terceiros, sem a anuência formal e expressa do TCU, das informações restritas reveladas.

4. 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 TCU, as informações restritas reveladas.

5. 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 TCU, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.

6. 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.

7. A EMPRESA RECEPTORA obriga-se a informar imediatamente ao TCU 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.

8. A quebra do sigilo das informações restritas reveladas, devidamente comprovada, sem autorização expressa do TCU, possibilitará a imediata rescisão de qualquer contrato firmado entre o TCU e a EMPRESA RECEPTORA sem qualquer ônus para o TCU. 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 TCU, inclusive os de ordem moral, bem como as de responsabilidades civil e criminal respectivas, as quais serão apuradas em regular processo judicial ou administrativo.

9. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de acesso às informações restritas do TCU.

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, ___ de _____ de 20__.

[NOME DA EMPRESA RECEPTORA]

_____ _____

Nome: Nome:

ANEXO VI – MODELO DE ORDEM DE SERVIÇO DE TREINAMENTO

TRIBUNAL DE CONTAS DA UNIÃO	**ORDEM DE SERVIÇO DE TREINAMENTO**
	Contrato nº XX/XXXX
	OST-AAAA-XXX

1. DESCRIÇÃO GERAL DOS SERVIÇOS/PRODUTOS (INCLUINDO AS EMENTAS E CARGA HORÁRIA)

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

2. PRAZO PARA EXECUÇÃO

Data de apresentação da documentação	Data de início	Data de término
XX/XX/XXXX	XX/XX/XXXX	XX/XX/XXXX

3. CRITÉRIOS DE AVALIAÇÃO DA QUALIDADE DOS SERVIÇOS/PRODUTOS

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

4. CUSTOS

Treinamento	Valor (R$)	Total (R$)
XXXXXXXXXXXXXX	XX,XX	XX,XX
XXXXXXXXXXXXXX	XX,XX	XX,XX
Total		XX,XX

5. PARTICIPANTES

Nome	Papel	E-mail	Telefone	Órgão/ Empresa
XXXXXXXXXXX	Responsável técnico da empresa	XXXXXXXXXXXX	xxxx-xxxx	Empresa x
XXXXXXXXXXX	Responsável técnico TCU	XXXXXXXXXXXX	xxxx-xxxx	TCU
XXXXXXXXXXX	Fiscalizador do contrato	XXXXXXXXXXXX	xxxx-xxxx	TCU

6. ANEXOS

Documento	Identificação
XXXXXXXXXXXXXX.XXX	CRONOGRAMA (Documento obrigatório)
XXXXXXXXXXXXXX.XXX	Plano de treinamento (Documento obrigatório)
XXXXXXXXXXXXXX.XXX	Material didático a ser utilizado (Documento obrigatório)
	"*Curriculum Vitae*" do instrutor (Documento obrigatório)
	Comprovantes de certificação do instrutor (Documento obrigatório)

7. São partes integrantes da Ordem de Serviço, o edital do Pregão Eletrônico nº 86/2011 e o contrato nº XX/XXXX, bem como cronograma de execução dos serviços e demais documentos em anexo.

Brasília, ____ de _____ de 20____.

Responsável técnico da empresa Empresa	Responsável técnico TCU TCU	Fiscalizador do contrato TCU

ANEXO VII – MODELO DE TERMO DE RECEBIMENTO DE SERVIÇOS DE TREINAMENTO

TRIBUNAL DE CONTAS DA UNIÃO	**TERMO DE RECEBIMENTO**
	Contrato nº XX/XXXX
	TR-OST-AAAA-XXX

1. DESCRIÇÃO GERAL DOS SERVIÇOS/PRODUTOS (INCLUINDO AS EMENTAS E CARGA HORÁRIA)

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

2. TREINAMENTOS REALIZADOS

Item	Descrição do serviço/produto	Data de Conclusão	Qtd. Horas
1.			
2.			
3.			
Total			

3. AVALIAÇÃO DA QUALIDADE DOS SERVIÇOS/PRODUTOS DE ACORDO COM OS CRITÉRIOS ESTABELECIDOS NA OST

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

4. VALORES A PAGAR (HOMOLOGADOS)

Treinamento	Valor (R$)	FATR (R$)	Total (R$)
XXXXXXXXXXXXXX	XX,XX	XX,XX	XX,XX
XXXXXXXXXXXXXX	XX,XX	XX,XX	XX,XX
Total			XX,XX

5. PARTICIPANTES

Nome	Papel	E-mail	Telefone	Órgão/ Empresa
XXXXXXXXXXX	Responsável técnico TCU	XXXXXXXXXXXX	xxxx-xxxx	TCU
XXXXXXXXXXX	Fiscalizador do contrato	XXXXXXXXXXXX	xxxx-xxxx	TCU

6. ANEXOS

Documento	Identificação
XXXXXXXXXXXXXX.XXX	Memória de cálculo do FATR (Documento obrigatório)
XXXXXXXXXXXXXX.XXX	

Brasília, ____ de ____________ de 20____.

Responsável técnico da empresa
Empresa

Responsável técnico TCU
TCU

Fiscalizador do contrato
TCU

ANEXO VIII – MODELO DE ORDEM DE SERVIÇO

TRIBUNAL DE CONTAS DA UNIÃO	**ORDEM DE SERVIÇO**
	Contrato nº XX/XXXX
	OS-AAAA-XXX

1. DESCRIÇÃO GERAL DOS SERVIÇOS/PRODUTOS

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

2. PRAZO PARA EXECUÇÃO

Data de início	Data de término	Número de dias úteis
XX/XX/XXXX	XX/XX/XXXX	

3. SERVIÇOS/PRODUTOS EXIGIDOS

Item	Descrição do serviço/produto	Data de Conclusão	Qtd. Horas
1.			
2.			
	Documento *as-built*		

Total			

4. SERVIÇOS/PRODUTOS NÃO EXIGIDOS

Item	Descrição do serviço/produto
1.	
2.	
3.	

5. CRITÉRIOS DE AVALIAÇÃO DA QUALIDADE DOS SERVIÇOS/PRODUTOS

6. CUSTOS

Perfil	Valor H/h (R$)	Qtd. Horas	Total (R$)
XXXXXXXXXXXXX	XX,XX	XXX	XX,XX
XXXXXXXXXXXXX	XX,XX	XXX	XX,XX
Total		XXX	XX,XX

7. PARTICIPANTES

Nome	Papel	E-mail	Telefone	Órgão/ Empresa
XXXXXXXXXX	Responsável técnico da empresa	XXXXXXXXXXX	xxxx-xxxx	Empresa x
XXXXXXXXXX	Responsável técnico TCU	XXXXXXXXXXX	xxxx-xxxx	TCU
XXXXXXXXXX	Fiscalizador do contrato	XXXXXXXXXXX	xxxx-xxxx	TCU

8. ANEXOS

Documento	Identificação
XXXXXXXXXXXXX.XXX	CRONOGRAMA (Documento obrigatório)

9. São partes integrantes da Ordem de Serviço, o edital do Pregão Eletrônico nº 86/2011 e o contrato nº XX/XXXX, bem como cronograma de execução dos serviços e demais documentos em anexo.

Brasília, ____ de _____ de 20____.

Responsável técnico
da empresa
Empresa

Responsável técnico TCU
TCU

Fiscalizador do contrato
TCU

ANEXO IX – MODELO DE TERMO DE RECEBIMENTO DE SERVIÇOS

TRIBUNAL DE CONTAS DA UNIÃO	**TERMO DE RECEBIMENTO**
	Contrato nº XX/XXXX
	TR-OS-AAAA-XXX

1. DESCRIÇÃO GERAL DOS SERVIÇOS/PRODUTOS

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

2. SERVIÇOS/PRODUTOS ENTREGUES

Item	Descrição do serviço/produto	Data de Conclusão	Qtd. Horas
1.			
2.			
3.			
Total			

3. AVALIAÇÃO DA QUALIDADE DOS SERVIÇOS/PRODUTOS DE ACORDO COM OS CRITÉRIOS ESTABELECIDOS NA OS

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

4. VALORES A PAGAR (HOMOLOGADOS)

Perfil	Valor H/h (R$)	Qtd. Horas	Valor total (R$)	FAEP (R$)	Total (R$)
XXXXXXXXXXXXXX	XX,XX	XXX	XX,XX	XX,XX	XX,XX
XXXXXXXXXXXXXX	XX,XX	XXX	XX,XX	XX,XX	XX,XX
Total					XX,XX

5. PARTICIPANTES

Nome	Papel	E-mail	Telefone	Órgão/ Empresa
XXXXXXXXXXX	Responsável técnico TCU	XXXXXXXXXXXX	xxxx-xxxx	TCU
XXXXXXXXXXX	Fiscalizador do contrato	XXXXXXXXXXXX	xxxx-xxxx	TCU

6. ANEXOS

Documento	Identificação
XXXXXXXXXXXXXX.XXX	Memória de cálculo do FAEP (Documento obrigatório)
XXXXXXXXXXXXXX.XXX	

Brasília, ____ de ____________ de 20____.

Responsável técnico da empresa
Empresa

Responsável técnico TCU
TCU

Fiscalizador do contrato
TCU

ANEXO X – MODELO DE DECLARAÇÃO DE VISTORIA

Declaro, em atendimento ao previsto no Edital de Pregão Eletrônico nº 86/2011, que eu, _____, portador(a) da CI/RG nº _____ e do CPF nº _____, representante da empresa _____, estabelecida no(a) _____ como seu(ua) representante legal para os fins da presente declaração, compareci perante o representante do Tribunal de Contas da União em Brasília e vistoriei o ambiente computacional do Tribunal assim como recebi o desenho esquemático da topologia de rede, tomando plena ciência das condições e grau de dificuldade existentes.

Local e data

_____
Assinatura
(Representante da empresa)

Visto:

_____
Representante do TCU

Observação:
1) Emitir em papel que identifique o licitante.

ANEXO XI - ATESTADO *(OU DECLARAÇÃO)* DE CAPACIDADE TÉCNICA

Atestamos *(ou declaramos)* que a empresa _____, inscrita no CNPJ (MF) nº _____, inscrição estadual nº _____, estabelecida no (a) _____, executa *(ou executou)* serviços de _____ para este órgão *(ou para esta empresa)*.

Atestamos *(ou declaramos)*, ainda, que os compromissos assumidos pela empresa foram cumpridos satisfatoriamente, nada constando em nossos arquivos que a desabone comercial ou tecnicamente.

Local e data

_____
Assinatura e carimbo do emissor

Observações:

1) Este atestado (ou declaração) deverá ser emitido em papel que identifique o órgão (ou empresa) emissor; e

2) o atestado (ou declaração) deverá estar visado pelo respectivo órgão fiscalizador, quando for o caso.

ANEXO XII – MINUTA DO CONTRATO

TERMO DE CONTRATO N.º _____ /20__ QUE ENTRE SI CELEBRAM A UNIÃO, POR INTERMÉDIO DO TRIBUNAL DE CONTAS DA UNIÃO, E _____ PARA O FORNECIMENTO DE SOLUÇÃO INTEGRADA DE SERVIÇOS GERENCIADOS DE SEGURANÇA COMPREENDENDO: PROVIMENTO DE SERVIÇOS DE SEGURANÇA; MONITORAMENTO E ADMINISTRAÇÃO DOS SERVIÇOS PROVIDOS; GESTÃO DE VULNERABILIDADES DA REDE TCU; RESPOSTA A INCIDENTES DE SEGURANÇA E TRANSFERÊNCIA DE CONHECIMENTO PARA A EQUIPE DO TRIBUNAL.

CONTRATANTE: A União, por intermédio do Tribunal de Contas da União[/se for o caso, indicar também o nome da Unidade Técnica], com sede no [inserir endereço completo], inscrito no CNPJ (MF) sob o n.º 00.414.607/____-__, representado pelo seu[inserir função da autoridade competente], Senhor(a) [inserir nome do titular ou substituto], de acordo com a [delegação/subdelegação]de competência contida no inciso _____ do art. _____ da Portaria da [Presidência ou Segedam] n.º _____, de _____.

CONTRATADA: _____, inscrita no CNPJ (MF) sob o n.º _____, estabelecida [inserir endereço completo], representada pelo seu [inserir cargo], Senhor(a) [inserir nome completo], portador(a) da Cédula de Identidade n.º _____ [inserir número e órgão expedidor/unidade da federação] e CPF (MF) n.º _____, de acordo com a representação legal que lhe é outorgada por [procuração/contrato social/estatuto social].

Os CONTRATANTES têm entre si justo e avençado, e celebram o presente contrato, instruído no TC n.º 018.969/2011-9 (Pregão Eletrônico 86/2011), mediante as cláusulas e condições que se seguem:

CLÁUSULA PRIMEIRA – DO OBJETO

1. O presente contrato tem como objeto o fornecimento de Solução Integrada de Serviços Gerenciados de Segurança compreendendo: provimento de serviços de segurança; monitoramento e administração dos serviços providos; gestão de vulnerabilidades da rede TCU; resposta a incidentes de segurança e transferência de conhecimento para a equipe do Tribunal, conforme tabela abaixo:

Item	Descrição
1	Serviços de *Firewall* Central Externo
2	Serviços de *Firewall* e *VPN* Central Interno
3	Serviços de *Firewall* e *VPN* Remoto

4	Serviços de Prevenção de Intrusão Central
5	Serviços de *Proxy/cache* com filtro de conteúdo *WEB*
6	Serviços de *SMTP Antispam*
7	Serviços de *Firewall* de Aplicação
8	Serviços de Consolidação e Correlacionamento de Eventos
9	Serviços de Gestão de Vulnerabilidades
10	Serviços de Monitoração e Administração de Segurança
11	Treinamentos
11.1	*Firewall* Central Externo
11.2	*Firewall* e *VPN* Central Interno
11.3	*Firewall* e *VPN* Remoto
11.4	Prevenção de Intrusão Central
11.5	*Proxy/cache* com filtro de conteúdo *WEB*
11.6	*SMTP Antispam*
11.7	*Firewall* de Aplicação
11.8	Consolidação e Correlacionamento de Eventos
11.9	Gestão de Vulnerabilidades
11.10	Monitoração e Administração de Segurança
12	Serviços Técnicos Especializados

CLÁUSULA SEGUNDA – DO VALOR

1. O valor total deste contrato é de R$ ____(___), conforme tabela a seguir:

Item	Descrição	Meses	Quant	Valor mensal/ unidade (R$)	Valor Total (R$)
1	Serviços de *Firewall* Central Externo	60	1		
2	Serviços de *Firewall* e *VPN* Central Interno	60	1		
3	Serviços de *Firewall* e *VPN* Remoto	56	29		
4	Serviços de Prevenção de Intrusão Central	53	2		
5	Serviços de *Proxy/cache* com filtro de conteúdo *WEB*	57	1		
6	Serviços de *SMTP Antispam*	57	1		
7	Serviços de *Firewall* de Aplicação	53	1		

8	Serviços de Consolidação e Correlacionamento de Eventos	60	1		
9	Serviços de Gestão de Vulnerabilidades	56	1		
10	Serviços de Monitoração e Administração de Segurança	60	1		
			Quant	**Valor unitário (R$)**	**Valor Total (R$)**
11	Treinamentos				
11.1	*Firewall* Central Externo		1		
11.2	*Firewall* e *VPN* Central Interno		1		
11.3	*Firewall* e *VPN* Remoto		1		
11.4	Prevenção de Intrusão Central		1		
11.5	*Proxy/cache* com filtro de conteúdo *WEB*		1		
11.6	*SMTP* (Antispam)		1		
11.7	*Firewall* de Aplicação		1		
11.8	Consolidação e Correlacionamento de Eventos		1		
11.9	Gestão de Vulnerabilidades		1		
11.10	Monitoração e Administração de Segurança		1		
12	Serviços Técnicos Especializados		1600		
TOTAL					

CLÁUSULA TERCEIRA – DA DESPESA E DOS CRÉDITOS ORÇAMENTÁRIOS

1. A despesa orçamentária da execução deste contrato correrá à conta da **Natureza da Despesa** _____, da **Atividade** _____, conforme Nota de Empenho n.º _____, de ___/___/____.

CLÁUSULA QUARTA – DOS PRAZOS DE EXECUÇÃO

1. Os prazos referentes à execução dos serviços (itens 1 a 12) deverão obedecer o disposto no Anexo II – Especificações Técnicas do Edital do Pregão Eletrônico n.º 86/2011.

CLÁUSULA QUINTA – DA VIGÊNCIA

1. O prazo de vigência deste contrato é de 60 (sessenta) meses, contado da data da sua assinatura, com eficácia após a publicação do seu extrato no Diário Oficial da União.

CLÁUSULA SEXTA – DA GARANTIA DO OBJETO

1. Todo o *hardware* a ser utilizado na prestação dos serviços deverá estar coberto pelo prazo de garantia estipulado pelo fabricante.

CLÁUSULA SÉTIMA – DA GARANTIA DE EXECUÇÃO DO CONTRATO

1. A CONTRATADA deverá apresentar à Administração do CONTRATANTE, no prazo máximo de 10 (dez) dias úteis, contado da data do protocolo de entrega da via do contrato assinada, comprovante de prestação de garantia correspondente ao percentual de 5% (cinco por cento) do valor total do contrato, pelo período correspondente à respectiva vigência contratual, podendo optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

2. A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

   2.1. Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

   2.2. Multas moratórias e punitivas aplicadas pela FISCALIZAÇÃO ao CONTRATADO;

   2.3. Obrigações trabalhistas não honradas pela AFIANÇADA; e

   2.4. Prejuízos causados à administração e/ou a terceiros decorrentes de culpa ou dolo durante a execução do contrato.

3. Não serão aceitas garantias na modalidade seguro-garantia em cujos termos não constem expressamente os eventos indicados nos itens 2.1 a 2.3 do item 2 imediatamente anterior.

   3.1. a contratada, em complementação ao seguro-garantia, também deverá apresentar seguro do ramo “responsabilidade civil”, correspondente ao percentual de 5% (cinco por cento) do valor global do contrato, destinado a cobrir eventuais prejuízos causados à administração e/ou a terceiros de que trata o subitem 2.4 do item 2 imediatamente anterior.

   3.2. tanto o seguro-garantia, como o seguro do ramo “responsabilidade civil”, considerados individualmente ou em conjunto, se prestarão a garantir no máximo 5% (cinco por cento) do valor anual atualizado do contrato.

      3.2.1. caso a Administração tenha de optar entre os 2 (dois) tipos de seguro, os riscos cobertos pelo seguro-garantia, em qualquer caso ou circunstâncias, terá prioridade em relação aos riscos cobertos pelo seguro do ramo “responsabilidade civil”.

4. A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal, em conta específica com correção monetária, em favor do Tribunal de Contas da União.

5. A garantia na modalidade fiança bancária deverá ser apresentada conforme o modelo constante no Anexo XIII.

6. A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,2% (dois décimos por cento) do valor do contrato por dia de atraso, até o máximo de 5% (cinco por cento).

7. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a retenção dos pagamentos devidos à CONTRATADA, até o limite de 5% (cinco por cento) do valor anual do contrato, a título de garantia.

7.1. A retenção efetuada com base no item 7 desta cláusula não gera direito a nenhum tipo de compensação financeira à CONTRATADA;

7.2. A CONTRATADA, a qualquer tempo, poderá substituir a retenção efetuada com base no item 7 desta cláusula por quaisquer das modalidade de garantia, caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária.

8. O garantidor deverá declarar expressamente que tem plena ciência dos termos do edital e das cláusulas contratuais.

9. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Tribunal de Contas da União com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

10. Será considerada extinta a garantia:

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

10.2. Com a extinção do contrato.

11. O Tribunal de Contas da União não executará a garantia na ocorrência de uma ou mais das seguintes hipóteses:

11.1. Caso fortuito ou força maior;

11.2. Alteração, sem prévio conhecimento da seguradora ou do fiador, das obrigações contratuais;

11.3. Descumprimento das obrigações pela CONTRATADA decorrentes de atos ou fatos praticados pela Administração;

11.4. Atos ilícitos dolosos praticados por servidores da Administração.

12. Caberá à própria Administração apurar a isenção da responsabilidade prevista nos itens 11.1 e 11.4 desta cláusula, não sendo a entidade garantidora parte no processo instaurado pelo Tribunal de Contas da União.

13. Não serão aceitas garantias que incluam outras isenções de responsabilidade que não as previstas nesta cláusula.

14. Para efeitos da execução da garantia, os inadimplementos contratuais deverão ser comunicados pelo CONTRATANTE à CONTRATADA e/ou à Instituição Garantidora, no prazo de até 90 (noventa) dias após o término de vigência do contrato.

CLÁUSULA OITAVA – DOS ENCARGOS DAS PARTES

1. As partes devem cumprir fielmente as cláusulas avençadas neste contrato, respondendo pelas consequências de sua inexecução total ou parcial.

2. A CONTRATADA, além das obrigações estabelecidas no Anexo II do Pregão Eletrônico n.º 86/2011, deve:

   2.1. nomear preposto para, durante o período de vigência, representá-lo na execução do contrato;

   2.2. manter, durante a vigência do contrato, as condições de habilitação exigidas na licitação, devendo comunicar ao CONTRATANTE a superveniência de fato impeditivo da manutenção dessas condições;

   2.3. reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções;

   2.4. responder pelos danos causados diretamente ao CONTRATANTE ou a terceiros, decorrentes de sua culpa ou dolo na execução do contrato;

   2.5. respeitar as normas de controle de bens e de fluxo de pessoas nas dependências do CONTRATANTE.

3. São expressamente vedadas à CONTRATADA:

   3.1. a veiculação de publicidade acerca deste contrato, salvo se houver prévia autorização do CONTRATANTE;

   3.2. a subcontratação para a execução do objeto deste contrato;

   3.3. a contratação de servidor pertencente ao quadro de pessoal do CONTRATANTE, durante a vigência deste contrato.

4. O CONTRATANTE, além das obrigações estabelecidas no Anexo II do Pregão Eletrônico n.º 86/2011, deve:

   4.1. prestar as informações e os esclarecimentos solicitados pela CONTRATADA para a fiel execução do contrato;

   4.2. receber o objeto;

   4.3. solicitar o reparo, a correção, a remoção, a reconstrução ou a substituição do objeto do contrato em que se verificarem vícios, defeitos ou incorreções.

CLÁUSULA NONA – DO RECEBIMENTO DA SOLUÇÃO

1. O recebimento definitivo dos serviços será realizado pela Secretaria de Infraestrutura de Tecnologia da Informação – Setic, conforme disposto no Anexo II do Pregão Eletrônico n.º 86/2011.

CLÁUSULA DÉCIMA – DO ACOMPANHAMENTO E DA FISCALIZAÇÃO

1. Durante a vigência deste contrato, a execução do objeto será acompanhada e fiscalizada pelo (a) titular da Secretaria de Infraestrutura de Tecnologia da Informação – Setic ou por representante do CONTRATANTE, devidamente designado para esse fim, permitida a assistência de terceiros.

2. Durante a vigência deste contrato, a CONTRATADA deve manter preposto, aceito pela Administração do CONTRATANTE, para representá-lo sempre que for necessário.

3. A atestação de conformidade do fornecimento do objeto cabe ao titular do setor responsável pela fiscalização do contrato ou a outro servidor designado para esse fim.

CLÁUSULA DÉCIMA PRIMEIRA – DA ALTERAÇÃO DO CONTRATO

1. Este contrato pode ser alterado nos casos previstos no art. 65 da Lei n.º 8.666/93, desde que haja interesse do CONTRATANTE, com a apresentação das devidas justificativas.

CLÁUSULA DÉCIMA SEGUNDA – DA REPACTUAÇÃO DOS PREÇOS DOS SERVIÇOS

1. É admitida repactuação deste Contrato, desde que seja observado o interregno mínimo de um ano.

2. O interregno mínimo de um ano para a primeira repactuação será contado a partir da data limite para a apresentação da proposta ou da data do orçamento a que a proposta se referir.

3. Nas repactuações subsequentes à primeira, o interregno de um ano será contado a partir da data de início dos efeitos financeiros da última repactuação ocorrida.

4. A CONTRATADA poderá exercer, perante o CONTRATANTE, seu direito à repactuação dos preços do contrato até a data da prorrogação contratual subsequente.

5. Caso a CONTRATADA não efetue de forma tempestiva a repactuação, ocorrerá a preclusão do direito de repactuar.

6. As repactuações serão precedidas de solicitação da CONTRATADA, acompanhada de demonstração analítica da alteração dos custos, por meio de apresentação das planilhas de custos e formação de preços, e, se for o caso, dos documentos indispensáveis à comprovação da alteração dos preços de mercado em cada um dos itens da planilha a serem alterados.

7. É vedada a inclusão, por ocasião da repactuação, de benefícios não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal, sentença normativa.

8. Quando da solicitação da repactuação, esta somente será concedida mediante negociação entre as partes, considerando-se:

8.1. os preços praticados no mercado e em outros contratos da Administração;

8.2. as particularidades do contrato em vigência;

8.3. a planilha com a variação dos custos apresentada;

8.5. indicadores setoriais, tabelas de fabricantes, valores oficiais de referencia, tarifas públicas ou outros equivalentes; e

8.6. a disponibilidade orçamentária do CONTRATANTE.

9. No caso de repactuação, será lavrado termo aditivo ao contrato vigente.

10. O CONTRATANTE poderá realizar diligências para conferir a variação de custos alegada pela CONTRATADA.

11. Os novos valores contratuais decorrentes da repactuação produzirão efeitos:

11.1. a partir da assinatura do termo aditivo;

11.2. em data futura, desde que acordada entre as partes, sem prejuízo da contagem de periodicidade para concessão das próximas repactuações futuras; ou

11.3. em data anterior à repactuação, exclusivamente quando a repactuação envolver revisão do custo de mão de obra e estiver vinculada a instrumento legal ou sentença normativa, podendo a data estipulada no instrumento para o início dos efeitos financeiros do reajuste salarial ser considerada para efeito de compensação do pagamento devido, assim como para a contagem da anualidade em repactuações futuras.

12. No caso do previsto no subitem 11.3, o pagamento retroativo deverá ser concedido exclusivamente para os itens que motivaram a retroatividade, e apenas em relação à diferença porventura existente.

13. O CONTRATANTE deverá assegurar-se de que os preços contratados são compatíveis com aqueles praticados no mercado, de forma a garantir a continuidade da contratação vantajosa.

14. O CONTRATANTE poderá prever o pagamento retroativo do período que a proposta de repactuação permaneceu sob sua análise, por meio de Termo de Reconhecimento de Dívida.

15. Na hipótese do item anterior, o período que a proposta permaneceu sob análise do CONTRATANTE será contado como tempo decorrido para fins de contagem da anualidade da próxima repactuação.

CLÁUSULA DÉCIMA TERCEIRA – DA RESCISÃO

1. A rescisão deste contrato se dará nos termos dos artigos 79 e 80 da Lei n.º 8.666/93.

1.1 No caso de rescisão provocada por inadimplemento da CONTRATADA, o CONTRATANTE poderá reter, cautelarmente, os créditos decorrentes do contrato até o valor dos prejuízos causados, já calculados ou estimados.

2. No procedimento que visa à rescisão do contrato, será assegurado o contraditório e a ampla defesa, sendo que, depois de encerrada a instrução inicial, a CONTRATADA terá o prazo de 5 (cinco) dias úteis para se manifestar e produzir provas, sem prejuízo da possibilidade de o CONTRATANTE adotar, motivadamente, providências acauteladoras.

CLÁUSULA DÉCIMA QUARTA – DA FUNDAMENTAÇÃO LEGAL E DA VINCULAÇÃO DO CONTRATO

1. O presente contrato fundamenta-se nas Leis nº 10.520/2002 e nº 8.666/1993 e vincula-se ao Edital e anexos do Pregão Eletrônico n.º 86/2011, constante do processo TC 018.969/2011-9, bem como à proposta da CONTRATADA.

CLÁUSULA DÉCIMA QUINTA – DA LIQUIDAÇÃO E DO PAGAMENTO

1. O CONTRATANTE realizará o pagamento, conforme estabelecido no Anexo II do Pregão Eletrônico n.º 86/2011.

2. O pagamento será realizado por meio de ordem bancária, creditada na conta corrente da CONTRATADA.

3. Nenhum pagamento será efetuado à CONTRATADA caso exista pendência de atestação de conformidade do serviço executado ou quanto às Fazendas Federal, Estadual e Municipal, incluída a regularidade relativa à Seguridade Social e ao Fundo de Garantia por Tempo de Serviço (FGTS).

3.1. O descumprimento, pela CONTRATADA, do estabelecido no item 3, não lhe gera direito a alteração de preços ou compensação financeira.

4. O CONTRATANTE pode deduzir do montante a pagar os valores correspondentes a multas, ressarcimentos ou indenizações devidas pela CONTRATADA, nos termos deste contrato.

5. No caso de atraso de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, serão devidos pelo CONTRATANTE, encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples.

5.1. O valor dos encargos será calculado pela fórmula: EM = I x N x VP, onde: EM = Encargos moratórios devidos; N = Números de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso.

CLÁUSULA DÉCIMA SEXTA – DAS SANÇÕES

1. A CONTRATADA será punida com o impedimento de licitar e contratar com a União, Estados, Distrito Federal ou Municípios e ser descredenciado no Sicaf e no cadastro de fornecedores do CONTRATANTE, pelo prazo de até 5 (cinco) anos, sem prejuízo das multas previstas neste contrato e demais cominações legais, nos seguintes casos:

1.1. apresentação de documentação falsa;

1.2. retardamento da execução do objeto;

1.3. falhar na execução do contrato;

1.4. fraudar na execução do contrato;

1.5. comportamento inidôneo;

1.6. declaração falsa;

1.7. fraude fiscal.

2. Para os fins do item 1.5, reputar-se-ão inidôneos atos tais como os descritos nos artigos 92, parágrafo único, 96 e 97, parágrafo único, da Lei n.º 8.666/1993.

2.1. Para condutas descritas nos itens 1.1, 1.4, 1.5, 1.6 e 1.7 será aplicada multa de no máximo 30% (trinta por cento) do valor do contrato.

3. Para os fins dos itens 1.2 e 1.3, será aplicada multa nas condições dispostas no Anexo II – Especificaçõs Técnicas do Edital do Pregão Eletrônico n.º 86/2011.

4. O valor da multa poderá ser descontado do pagamento a ser efetuado à CONTRATADA.

4.1. Se o valor a ser pago à CONTRATADA não for suficiente para cobrir o valor da multa, a diferença será descontada da garantia contratual.

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

4.3. Esgotados os meios administrativos para cobrança do valor devido pela CONTRATADA ao CONTRATANTE, este será encaminhado para inscrição em dívida ativa.

4.4. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento da multa, esta deve ser complementada no prazo de até 10 (dias) dias úteis, contado da solicitação do CONTRATANTE, a partir do qual se observará o disposto nos itens 6 e 7 da cláusula sétima deste contrato.

CLÁUSULA DÉCIMA SÉTIMA – DO FORO

1. As questões decorrentes da execução deste instrumento, que não possam ser dirimidas administrativamente, serão processadas e julgadas na Justiça Federal, no Foro da cidade de Brasília, Seção Judiciária do Distrito Federal, com exclusão de qualquer outro, por mais privilegiado que seja, salvo nos casos previstos no art. 102, inciso I, alínea “d”, da Constituição Federal.

E, para firmeza e validade do que foi pactuado, lavrou-se o presente Contrato em 2 (duas) vias de igual teor e forma, para que surtam um só efeito, as quais, depois de lidas, são assinadas pelos representantes das partes, CONTRATANTE e CONTRATADA, e pelas testemunhas abaixo.

Brasília - DF, em [data].

TRIBUNAL DE CONTAS DA UNIÃO

[Nome da autoridade competente]
[inserir nome do cargo]

CONTRATADA

Representante
Procurador/cargo

TESTEMUNHAS:

_____	_____
NOME:	NOME:
CPF:	CPF:
RG:	RG:

ANEXO XIII – MODELO DE CARTA DE FIANÇA BANCÁRIA PARA GARANTIA DE EXECUÇÃO CONTRATUAL

1. Pela presente, o (a) _____ (nome da instituição fiadora) com sede em _____ (endereço completo), por seus representantes legais infra-assinados, declara que se responsabiliza como FIADOR e principal pagador, com expressa renúncia dos benefícios estatuídos no Artigo 827, do Código Civil Brasileiro, da empresa _____ (nome da empresa), com sede em _____ (endereço completo), até o limite de R$ _____ (valor da garantia) (_____) (valor por escrito) para efeito de garantia à execução do Contrato nº _____ (número do contrato, formato xx/ano), decorrente do processo licitatório _____ (modalidade e número do instrumento convocatório da licitação – ex.: PE nº xx/ano), firmado entre a AFIANÇADA e o Tribunal de Contas da União para _____ (objeto da licitação), tendo este FIADOR plena ciência dos termos do referido Edital licitatório e das cláusulas contratuais.

2. A fiança ora concedida visa garantir o cumprimento, por parte de nossa AFIANÇADA, de todas as obrigações estipuladas no contrato retromencionado, abrangendo o pagamento de:

a) prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

b) prejuízos causados à Administração contratante ou a terceiro, decorrentes de culpa ou dolo durante a execução do contrato;

c) multas moratórias e punitivas aplicadas pela Administração contratante à AFIANÇADA; e

d) obrigações trabalhistas não honradas pela AFIANÇADA.

3. Esta fiança é valida por _____ (prazo, contado em dias, correspondente à vigência do contrato) (_____) (valor por escrito) dias, contados a partir de _____ (data de início da vigência do contrato), vencendo-se, portanto em _____ (data).

4. Na hipótese de inadimplemento de qualquer das obrigações assumidas pela AFIANÇADA, o (a) _____ (nome da instituição fiadora) efetuará o pagamento das importâncias que forem devidas, no âmbito e por efeito da presente fiança, até o limite acima estipulado, no prazo de 48 (quarenta e oito) horas, contado do recebimento de comunicação escrita do Tribunal de Contas da União.

5. A comunicação de inadimplemento deverá ocorrer até o prazo máximo de 90 (dias) após o vencimento desta fiança.

6. Nenhuma objeção ou oposição da nossa AFIANÇADA será admitida ou invocada por este FIADOR com o fim de escusar-se do cumprimento da obrigação assumida neste ato e por este instrumento perante o Tribunal de Contas da União.

7. Obriga-se este FIADOR, outrossim, pelo pagamento de quaisquer despesas judiciais e/ou extrajudiciais, bem assim por honorários advocatícios, na hipótese do Tribunal de Contas da União se ver compelido a ingressar em juízo para demandar o cumprimento da obrigação a que se refere a presente fiança.

8. Se, no prazo máximo de 90 (noventa) dias após a data de vencimento desta fiança, o (a) _____ (nome da instituição fiadora) não tiver recebido do Tribunal de Contas da União qualquer comunicação relativa a inadimplemento da AFIANÇADA, ou termo circunstanciado de que a AFIANÇADA cumpriu todas as cláusulas do contrato, acompanhado do original desta Carta de Fiança, esta fiança será automaticamente extinta, independentemente de qualquer formalidade, aviso, notificação judicial ou extrajudicial, deixando, em consequência, de produzir qualquer efeito e ficando o FIADOR exonerado da obrigação assumida por força deste documento.

9. Declara, ainda, este FIADOR, que a presente fiança está devidamente contabilizada e que satisfaz às determinações do Banco Central do Brasil e aos preceitos da legislação bancária aplicáveis e, que, os signatários deste Instrumento estão autorizados a prestar a presente fiança.

10. Declara, finalmente, que está autorizado pelo Banco Central do Brasil a expedir Carta de Fiança e que o valor da presente se contém dentro dos limites que lhe são autorizados pela referida entidade federal.

(Local e data)

(Instituição garantidora)

(Assinaturas autorizadas)