EDITAL Nº 2/2018
PREGÃO ELETRÔNICO
SISTEMA DE REGISTRO DE PREÇOS

PROCESSO Nº	**51402.180668/2017-96**
MODALIDADE:	**PREGÃO ELETRÔNICO**
CRITÉRIO DE JULGAMENTO (itens / grupos)	**MENOR VALOR GLOBAL POR LOTE**
REGIME DE EXECUÇÃO	**INDIRETA POR PREÇO UNITÁRIO**
UASG DA VALEC	**275075**
ABERTURA	**16/03/2018**
HORÁRIO	**10h**
OBJETO	Aquisição de Plataforma de Segurança com funcionalidade de proteção à rede, usuários/servidores críticos e inteligência no combate a ameaças, incluindo o fornecimento de equipamentos e softwares integrados em forma de appliance e/ou software appliance (módulo virtual) quando especificado, serviços de instalação e configuração, suporte técnico e garantia e transferência de conhecimento.
VALOR ESTIMADO:	**R$ 22.990.412,99** (vinte e dois milhões, novecentos e noventa mil, quatrocentos e doze reais e noventa e nove centavos)**.**
AMPLA CONCORRÊNCIA	

O Edital estará disponível para consulta e retirada nos sites: www.valec.gov.br e www.comprasgovernamentais.gov.br.

A **VALEC** não se responsabilizará pelos editais, possíveis planilhas, formulários e demais informações, obtidos ou conhecidos de forma ou em local diverso do disposto acima.

EDITAL Nº 2/2018
PREGÃO ELETRÔNICO
SISTEMA DE REGISTRO DE PREÇOS

A **VALEC Engenharia Construções e Ferrovias S/A**, torna público, para conhecimento dos interessados, que na data, horário e local acima indicados realizará licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA**, para **REGISTRO DE PREÇOS,** conforme acima indicado.

O procedimento licitatório obedecerá integralmente às seguintes legislações: Lei nº 10.520/2002; Decreto nº 3.555/2000; Decreto nº 5.450/2005; Decreto nº 3.722/2001; Lei Complementar nº 123/2006; Decreto nº 6.204/2007; Decreto nº 7.174/2010; Decreto nº 8.538/2015; Decreto nº 8.186/2014; Decreto nº 7.892/2013; Instrução Normativa Nº 01/2010 – SLTI/MPOG (Sustentabilidade); Instrução Normativa Nº 02/2010 – SLTI/MPOG (SICAF), Instrução Normativa nº 04/2014 –SLTI/MPOG; Instrução Normativa nº 005/2017 – SLTI/MPOG e, subsidiariamente, às disposições da Lei nº 8.666 de 21 de junho de 1993, e alterações posteriores, bem como o Regulamento Interno de Licitações e Contratos – RILC/VALEC em conformidade com a autorização contida no Processo Administrativo acima referenciado.

1. DO OBJETO:

1.1 Registro de Preços para eventual Aquisição de Plataforma de Segurança com funcionalidade de proteção à rede, usuários/servidores críticos e inteligência no combate a ameaças, incluindo o fornecimento de equipamentos e softwares integrados em forma de appliance e/ou software appliance (módulo virtual) quando especificado, serviços de instalação e configuração, suporte técnico e garantia e transferência de conhecimento.

2. DOS ANEXOS:

2.1. Anexo 1 – Termo de Referência;

2.1.1 Anexo I – Especificações técnicas (Neste anexo, incluído Modelo de Proposta de Preços);

2.1.2 Anexo II– Modelo de questionário de satisfação da Transferência de Conhecimento;

2.1.3 Anexo III – Atendimento às especificações;

2.1.4 Anexo IV – Penalidades e multas;

2.1.5 Anexo V – Termo de aceite provisório;

2.1.6 Anexo VI – Termo de aceite definitivo;

2.1.7 Anexo VII – Ordem de recebimento de bens:

2.1.8 Anexo VIII – Modelo de atestado;

2.1.9 Anexo IX – Termo de ciência;

2.1.10 Anexo X – Termo de compromisso.

2.2. Anexo 2 – Minuta de Contrato;

2.3. Anexo 3 – Minuta da Ata de Registro de Preços.

3. DA DOTAÇÃO ORÇAMENTÁRIA:

3.1 Conforme artigo 7º, § 2º do Decreto nº 7.892, de 23 de janeiro de 2013, na licitação para Registro de Preços, não é necessário indicar a dotação orçamentária, que somente será exigida para a formalização do contrato ou outro instrumento hábil.

4. DO SISTEMA DE REGISTRO DE PREÇOS:

4.1. O órgão gerenciador é a **VALEC Engenharia Construções e Ferrovias S/A,** tendo como participante o Departamento Nacional de Infraestrutura de Transportes – DNIT, com os seguintes quantitativos:

GRUPO 1 – SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO FÍSICO				
ITEM	**DESCRITIVO**	**REQUISIÇÃO INICIAL VALEC**	**REQUISIÇÃO INICIAL DNIT**	**REQUISIÇÃO INICIAL TOTAL**
1	Módulo de controle de perímetro físico	2	2	**4**
2	Módulo de proteção à usuários e servidores críticos	1.200	5000	**6200**
3	Módulo de inteligência no combate à ameaças	1	1	**2**
4	Suporte técnico dos módulos de proteção de perímetro físico	1	1	**2**
GRUPO 2 – SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO VIRTUAL				
ITEM	**DESCRITIVO**	**REQUISIÇÃO INICIAL VALEC**	**REQUISIÇÃO INICIAL DNIT**	**REQUISIÇÃO INICIAL TOTAL**
5	Módulo de controle de perímetro virtual	4	0	**4**
6	Módulo de gerência centralizado	1	0	**1**
7	Suporte técnico dos módulos de proteção e gerência centralizada do perimetro virtual	1	0	**1**

Grupo = Lote

4.2. A ata de registro de preços, durante sua validade, poderá ser utilizada por qualquer órgão ou entidade da administração pública que não tenha participado do certame licitatório, mediante anuência da VALEC, desde que devidamente justificada a

vantagem e respeitadas, no que couber, as condições e as regras estabelecidas na Lei nº 8.666/93 e no Decreto nº 7.892/13.

4.3. As adesões à ata de registro de preços são limitadas, na totalidade, no máximo ao quíntuplo do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independente do número de órgãos não participantes que eventualmente aderirem.

4.4. Para a utilização da Ata de Registro de Preços, deverão ser observadas as determinações contidas no artigo 22 do Decreto nº 7.892/13.

5. DO CREDENCIAMENTO:

5.1. O cadastro no SICAF poderá ser iniciado no Portal de Compras do Governo Federal, no sítio www.comprasgovernamentais.gov.br, com a solicitação de login e senha pelo interessado. Para efeitos deste item, VALEC não é unidade cadastradora do SICAF.

5.2. O credenciamento junto ao provedor do sistema implica a responsabilidade do licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes a este Pregão.

6. DAS CONDIÇÕES DE PARTICIPAÇÃO:

6.1. Poderão participar do presente procedimento licitatórios as interessadas cujo ramo de atividade seja compatível com o objeto desta licitação, que atendam às exigências, inclusive quanto à documentação, constantes deste Edital e seus Anexos e que estejam com Credenciamento regular no Sistema de Cadastramento Unificado de Fornecedores – SICAF, conforme disposto no art. 8º, § 3º da Instrução Normativa nº 02/2010-MPOG.

6.2. Para fins de verificação da manutenção do enquadramento da ME/EPP, o Pregoeiro consultará o portal da Transparência do Governo Federal (www.portaldatransparencia.gov.br), para verificar se o total dos valores recebidos no exercício anterior, extrapola o limite de R$ 3.600.000,00 (três milhões e seiscentos mil reais) previsto no art. 3º, inciso II, da Lei Complementar 123/06, ou o limite proporcional de que trata o art. 3º, § 2º, do mesmo diploma, em caso de início de atividade no exercício considerado.

6.2.1. A consulta também abrangerá o exercício corrente, para verificar se o total dos valores recebidos, até o mês anterior ao da sessão pública da licitação, extrapola os limites acima referidos, acrescidos do percentual de 20% (vinte por cento) de que trata o art. 3º, §§9º- A e 12, da Lei Complementar 123/2006.

6.2.2. Constatada a ocorrência de qualquer das situações que extrapolem o limite legal, o Pregoeiro indeferirá a aplicação do tratamento diferenciado em favor do licitante, conforme artigo 3º, §§ 9º-A, 10 e 12, da Lei Complementar 123/2006, com a consequente recusa do lance de desempate, sem prejuízo das penalidades incidentes.

6.3. Será permitida a subcontratação para a execução dos serviços e fornecimento de bens somente de empresas pertencentes à rede autorizada do fabricante dos sistemas.

6.3.1 Será observado o limite de subcontratação em 30% do valor do lote.

6.4. Além dos casos previstos no artigo 9º da Lei nº 8.666/1993, **não** poderá participar do presente Pregão o licitante que:

6.4.1. Esteja reunido sob a forma de consórcio ou cooperativas de empresas, quaisquer que sejam suas formas de constituição;

6.4.2. Tenha sofrido decretação de falência, dissolução, concurso de credores, concordata ou insolvência, bem como aquele que esteja em processo de liquidação, recuperação judicial ou extrajudicial;

6.4.3. Se encontre em recuperação judicial ou extrajudicial e não apresente Plano de Recuperação aprovado e homologado judicialmente e com a recuperação já deferida, conforme Parecer Nº 04/2015/CPLC/DEPCONSU/PGF/AGU. O pregoeiro submeterá o Plano de Recuperação e/ou qualquer outro documento encaminhado para fins de comprovação ou justificativa à Assessoria Jurídica para análise e Parecer.

6.4.4. Que tenham sido declaradas inidôneas para licitar ou contratar com a Administração Pública ou com qualquer de seus órgãos descentralizados, nos termos do artigo 7º da Lei 10.520/2002, e subsidiariamente do art. 87 da Lei 8.666/93, conforme consulta nos seguintes cadastros:

a) Cadastro Nacional de Empresas Inidôneas e Suspensas – CEIS;
b) Certidão Negativa de Inidôneos emitida pelo Tribunal de Contas da União – CNI/TCU;
c) Sistema de Cadastramento Unificado de Fornecedores – SICAF;
d) Cadastro Nacional de Condenações Cíveis por Ato de Improbidade Administrativa do Conselho Nacional de Justiça.

6.4.5. Esteja cumprindo a penalidade de suspensão temporária de participação em licitação e impedimentos de contratar com a Administração Pública Federal ou entidades vinculadas (Acórdão 2081/2014 – Plenário/TCU). Será considerado o âmbito de abrangência da penalidade, desde que devidamente registrado nos cadastros acima indicados.

6.4.6. Possua em seu contrato ou estatuto social finalidade ou objeto incompatível com o deste Pregão Eletrônico;

7. DOS ESCLARECIMENTOS E IMPUGNAÇÕES:

7.1. Qualquer esclarecimento em relação ao Edital e seus Anexos deverá ser encaminhado, por escrito, em até 03 (três) dias úteis anteriores à data fixada para abertura da sessão pública, ao Pregoeiro, no endereço eletrônico: gelic@valec.gov.br, devendo ser informado no campo "Assunto", a modalidade e o número da licitação **(Edital nº 2/2018 - Pregão Eletrônico),** observado o horário de funcionamento da VALEC, de 8h às 18h.

7.1.1. Esclarecimentos enviados fora do horário indicado, no último dia do prazo, serão considerados intempestivos e não serão respondidos.

7.1.2. As respostas serão divulgadas exclusivamente no site Comprasnet e em eventuais Cadernos de Perguntas e Respostas a serem disponibilizados no endereço eletrônico www.valec.gov.br e se vinculam ao Edital.

7.1.3. DÚVIDAS SOBRE O COMPRASNET: As dúvidas acerca da operacionalização do sistema Comprasnet deverão ser esclarecidas junto à **Central de Serviços do Serpro** por meio do telefone **0800-9789001**.

7.1.4. Os possíveis cadernos de perguntas e respostas publicados nos sites www.valec.gov.br e www.comprasnet.gov.br, vinculam o Edital e é de obrigatória observância pelos licitantes

7.2. Até 02 (dois) dias úteis antes da data fixada para recebimento das propostas, qualquer pessoa física ou jurídica poderá impugnar o ato convocatório deste Pregão:

7.2.1. A(s) impugnação(ões) deverá(ão) ser encaminhada(s) à Gerência de Licitações – GELIC, pelo e-mail: gelic@valec.gov.br, no horário de 8h às 18h.

7.2.2. Impugnações enviadas fora do horário indicado, no último dia do prazo, serão consideradas intempestivas e não serão conhecidas.

7.2.3. As impugnações enviadas em nome de Pessoa Jurídica deverão ser acompanhadas de cópia do contrato social e se protocolada por representante, incluir-se-á procuração, sempre com a documentação de identificação do outorgado.

7.2.4. As impugnações protocoladas de forma diversa da estipulada acima ou interpostas fora do prazo legal estabelecidos, não serão acatadas.

7.2.5. Caberá ao Pregoeiro, decidir sobre a impugnação no prazo de até 24h (vinte e quatro horas).

7.2.6. Acolhida a impugnação será designada uma nova data para a abertura do certame.

8. DO CADASTRO DAS PROPOSTAS:

8.1. O licitante deverá, até a abertura da sessão pública, cadastrar a sua Proposta no Comprasnet nos itens/grupos que forem de seu interesse, manifestando em campo próprio do sistema eletrônico a descrição detalhada do objeto ofertado, de forma mínima, sem identificação do proponente, bem como preencher as demais declarações que se fizerem necessárias.

8.1.1. Em caso de participação em grupos, deverá oferecer proposta para todos os itens que o compõem.

8.2. O cadastro da Proposta no Comprasnet implica a aceitação integral e irretratável dos termos do presente Edital, não sendo admitidas alegações de desconhecimento de fatos e condições que impossibilitem ou dificultem a execução do objeto licitado.

9. DO PROCEDIMENTO LICITATÓRIO:

9.1. Na data e horário previstos no preâmbulo, terá início a sessão pública do presente certame, com a divulgação das Propostas de Preços recebidas e início da etapa de lances, conforme Edital e de acordo com o Decreto nº 5.450/05.

9.2. Incumbe ao licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão e possíveis mensagens que sejam enviadas até a homologação final do certame, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de quaisquer mensagens emitidas pelo sistema ou de sua desconexão, sendo responsável por todas as transações que forem efetuadas em seu nome no sistema eletrônico.

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

9.4. Após a abertura da sessão, o Pregoeiro poderá suspendê-la, adiá-la ou reabri-la a qualquer momento, informando previamente os Licitantes por meio do Chat.

9.5. O Pregoeiro verificará as propostas apresentadas, desclassificando desde logo aquelas que não estejam em conformidade com os requisitos estabelecidos neste Edital, ou que contenham identificação do proponente.

9.6. No caso de eventual empate entre propostas, o sistema promoverá automaticamente sua ordenação.

9.6.1. Se permanecerem empatadas, pois as propostas foram dadas em tempos exatamente iguais, o pregoeiro poderá propor às empresas com propostas empatadas, um desempate, condicionado ao envio de um único lance via chat. Aquela que ofertar o menor lance, será a ganhadora, sendo que o valor deste lance que desempatou o certame, será inserido, na fase de Aceitação, no campo "Valor Negociado", com a devida justificativa.

9.6.2. Se nenhuma empresa convocada para o desempate quiser ofertar o lance ou se por casualidade, o lance for o mesmo, o pregoeiro deverá proceder novamente o procedimento anterior, via chat, até obter o desempate.

DA FASE DE LANCES:

9.7. Iniciada a fase de lances a ser realizada exclusivamente por meio do Sistema Comprasnet, serão observadas as seguintes regras:

9.7.1. Os lances deverão ser formulados sucessivamente de acordo com o valor de cada item/grupo licitado.

9.7.2. O licitante somente poderá oferecer lance inferior ao último por ele ofertado, ainda que superior ao menor registrado no sistema;

9.7.3. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar;

9.7.4. Serão excluídos pelo Pregoeiro os lances considerados simbólicos, irrisórios ou de valor igual a zero, incompatíveis com os praticados no mercado e com os custos estimados para a execução do objeto.

9.8. No caso de desconexão do Pregoeiro, no decorrer da etapa de lances, se o sistema eletrônico permanecer acessível aos licitantes, os lances continuarão sendo recebidos, sem prejuízo dos atos realizados.

9.9. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão será suspensa e reiniciada somente após comunicação prévia e expressa do Pregoeiro aos Licitantes no Comprasnet.

9.10. A etapa competitiva será encerrada a qualquer momento, mediante Aviso de Iminência, emitido pelo sistema eletrônico aos licitantes, após o que, transcorrerá período de tempo de até 30 (trinta) minutos determinado, também, pelo sistema eletrônico, findo o qual será automaticamente encerrada a recepção de lances.

9.11. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta e, na hipótese de desistência de apresentar outros lances, valerá o último lance por ele ofertado, para efeito de ordenação das propostas.

9.12. Para a contratação de serviços comuns de informática e automação, definidos no art. 16-A da Lei n° 8.248/91, será assegurado o direito de preferência previsto no seu artigo 3º, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174/10.

9.12.1. Quando aplicada a margem de preferência a que se refere o Decreto nº 7.546/11, não se aplicará o sorteio previsto no Decreto nº 7.174/10.

9.13. Nas contratações de serviços de informática e automação, nos termos da Lei nº 8.248, de 1991, as licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

9.14. Caso o sistema não emita o aviso de fechamento iminente, o Pregoeiro se responsabilizará pelo aviso de encerramento as licitantes.

9.15. Encerrada a fase de lances, se o melhor lance não tiver sido ofertado por ME/EPP e houver lance de ME/EPP de porte igual ou superior em até 5% (cinco por cento) àquele, proceder-se-á a fase de desempate. (art. 44 da Lei Complementar 123/2006).

9.16. O sistema convocará a ME/EPP para, no prazo de 5 (cinco) minutos, controlados pelo Sistema, encaminhar uma última oferta, obrigatoriamente abaixo da primeira colocada para o desempate.

9.17. Caso a ME/EPP não oferecer valor inferior, o sistema convocará as licitantes ME/EPP remanescentes que porventura se enquadrem na mesma condição, seguindo-se a ordem de classificação para o exercício do mesmo direito.

9.18. Caso o sistema convoque todas as ME/EPP e estas deixem de ofertar menor valor, o Pregoeiro convocará o próximo licitante para ofertar melhor lance, prosseguindo-se a sessão pública.

9.19. Encerrada a fase de lances, o Pregoeiro verificará as condições de participação do licitante classificado em primeiro lugar e, estando em conformidade, iniciará a etapa de negociação de preços via chat, com o fim de obter proposta mais vantajosa por meio de

contraproposta, podendo ser acompanhada pelos demais licitantes, vedada a negociação em condições diversas das previstas neste Edital.

9.20. O licitante classificado em primeiro lugar deverá enviar pelo Sistema Comprasnet, via Convocação de Anexo, **no prazo mínimo de 2h** (duas horas), a contar da convocação, a Proposta de Preços e Documentação de Habilitação, devidamente atualizados, em conformidade com o último lance ofertado, indicando expressamente a marca que será fornecida.

9.20.1. A critério do Pregoeiro, poderá ser concedido prazo superior ao mínimo estabelecido, bem como poderá ser solicitado o envio somente da Proposta de Preços e posteriormente, via nova convocação, o envio da documentação de habilitação.

9.21. O não atendimento da convocação referida no subitem anterior acarretará na desclassificação da proposta.

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

9.23. É facultado ao Pregoeiro a realização de diligência destinada a esclarecer ou a confirmar a veracidade das informações, prestadas pelo Licitante, constantes de sua Proposta e de eventuais documentos a ela anexados.

DAS HIPÓTESES DE DESCLASSIFICAÇÃO:

9.24. Será desclassificado o licitante que:

a) Após diligência realizada pelo Pregoeiro nos sítios oficiais, constatar o desenquadramento da condição de ME/EPP;

b) Não atender qualquer solicitação realizada pelo Pregoeiro, via chat, no prazo estabelecido;

c) Deixar, injustificadamente, de cumprir a diligência solicitada pelo Pregoeiro;

d) Deixar, injustificadamente, de responder à convocação via chat realizada pelo Pregoeiro;

e) Enviar a documentação por meio divergente do solicitado pelo Pregoeiro;

f) Não enviar a documentação pela ferramenta “Convocar Anexo” no prazo estabelecido pelo Pregoeiro;

g) Não mantiver sua proposta após a data e hora da abertura do certame, sob pena das sanções previstas no art. 7º da Lei nº 10.520/2002.

9.25. Será desclassificado o licitante que apresentar a Proposta de Preços que:

a) Esteja em desacordo com o Edital;

b) Apresentem irregularidades insanáveis;

c) Majorar itens não elencados para correção em diligência

d) Cujos valores global e/ou unitários sejam superiores ao limite estabelecido no Termo de Referência;

e) Cujos valores forem inexequíveis, assim considerados aqueles que não tenham sua viabilidade demonstrada pelo Licitante;

9.26. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

9.27. Se a proposta ou lance vencedor for desclassificado, o Pregoeiro examinará a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação, podendo negociar com o licitante para obtenção de melhor proposta.

9.28. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

9.29. Eventual alegação de problemas, indisponibilidade, dificuldade, relativos ao Sistema, deverão ser comprovados pelo licitante por meio de documento emitido pelo provedor do mesmo (SERPRO).

9.30. Caso julgue necessário, o Pregoeiro poderá solicitar à licitante classificada em primeiro lugar que evidencie a exequibilidade de seu lance ofertado, por meio de justificativas e documentos, os quais serão encaminhados para análise da área requisitante, a fim de que possa emitir parecer acerca da exequibilidade, caso apresentem preços global e/ou unitários simbólicos, irrisórios ou incompatíveis com os preços dos insumos e valores de mercado, acrescidos dos respectivos encargos, ainda que o Edital não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio licitante, para os quais ele renuncie a parcela ou à totalidade da remuneração.

9.31. A Proposta considerada inexequível será recusada pelo Pregoeiro, hipótese em que será convocado o próximo colocado, podendo negociar melhor valor para fins de aceitação.

10. DA PROPOSTA DE PREÇOS:

10.1. A proposta vencedora deverá ser emitida em papel timbrado que identifique o licitante, sem emendas, rasuras ou entrelinhas. A proposta deverá estar datada e assinada por seu Representante Legal ou Procurador, com indicação de número da cédula de identidade, órgão emissor, número de CPF e o cargo por ele ocupado na empresa e ainda deverá conter:

a) O número do Pregão Eletrônico para Sistema de Registro de Preço, data e hora da sua realização;

b) O nome, a razão social da licitante, CNPJ, endereço, telefones, fax, endereços eletrônicos e funcionário de contato;

c) O prazo de validade não inferior a 120 (cento e vinte) dias, contados da data de abertura do presente Pregão Eletrônico;

d) Documentos que contenham a especificação técnica detalhada do objeto;

e) Todas as características técnicas obrigatórias deverão ser do fabricante e comprovadas por meio de folders, ou catálogos, ou manuais, ou impressão de páginas do fabricante na Internet, os quais deverão ser entregues juntamente com a proposta de preços;

f) O preço ofertado deverá ser expresso em REAL (R$), limitado a 02 casas decimais, devendo ser desprezadas as demais;

g) A planilha abaixo indicada devidamente preenchida:

LOTE	ITEM	DESCRIÇÃO DOS ITENS	QTD VALEC	QTD DNIT	QTD TOTAL	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
1 - Solução de Proteção de Perímetro Físico	1	Módulo de controle de perímetro físico	2	2	4	Hardware		
1 - Solução de Proteção de Perímetro Físico	2	Módulo de proteção à usuários e servidores críticos	1200	5000	6.200	Licença		
1 - Solução de Proteção de Perímetro Físico	3	Módulo de inteligência no combate à ameaças	1	1	2	Licença		
1 - Solução de Proteção de Perímetro Físico	4	Suporte técnico dos módulos de proteção de perímetro físico	1	1	2	Serviço		
2 - Solução de Proteção de Perímetro Virtual	5	Módulo de controle de perímetro virtual	4	0	4	Software		
2 - Solução de Proteção de Perímetro Virtual	6	Módulo de gerência centralizado	1	0	1	Sofware		
2 - Solução de Proteção de Perímetro Virtual	7	Suporte técnico dos módulos de proteção e gerência centralizada do perimetro virtual	1	0	1	Serviço		

h) Para fins de cálculo da planilha, somente serão consideradas 2 (duas) casas decimais, sendo as demais desconsideradas, não sendo permitido o arredondamento.

i) Declaração expressa, de que nos preços cotados estão incluídas todas as despesas relativas à entrega dos produtos adquiridos ou realização dos serviços nos locais discriminados no Termo de Referência, bem como de todos os tributos e encargos de qualquer natureza que, direta ou indiretamente, incidam sobre o valor do eventual fornecimento;

j) Os dados bancários para recebimento (pagamento) em nome da licitante: Nome e número do Banco, agência e conta corrente.

k) Documento denominado "Atendimento às Especificações" (modelo constante do Anexo III do Termo de Referência) para demonstrar o atendimento aos subitens constantes no **item 3 "Especificação Técnica";**

l) Eventuais Memórias de Cálculo que se fizerem necessárias;

m)Caso a proposta seja assinada por representante da empresa, esta deverá estar acompanhada de cópia de procuração por instrumento público e de cópia de documento de identificação do procurador.

10.2. Juntamente com a Proposta, a licitante deverá enviar **comprovante (declaração) de que é fabricante da Solução ou subsidiária brasileira do fabricante ou, ainda, que está credenciada pelo fabricante/subsidiária a comercializar licenças e implantar no Brasil o software/hardware ofertado, bem como autorizada a conceder o direito de utilização do produto contratado,** conforme item 14.2.3 do Termo de Referência e ainda de que é **revenda autorizada de seus produtos, e que está apta a executar os serviços de instalação e suporte técnico, conforme itens 14.2.3e 30.1.3 do Termo de Referência.**

10.3. A licitante **deverá identificar na Proposta Comercial, ao menos dois profissionais certificados pelo fabricante da solução**, estando esses aptos e autorizados a instalar, configurar e prestar manutenção nos equipamentos e softwares fornecidos, conforme item 14.2.4 do Termo de Referência.

10.4. O atendimento os item 10.2 e 10.3 deve ser comprovado por meio de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa, conforme tabela abaixo (item 14.2.5 do Termo de Referência). O não atendimento destes requisitos implicará na desclassificação da proposta.

Item	Link	Documento	Página	Localização

10.5. A Proposta de Preços acrescida da documentação técnica exigida no edital deverá estar numerada sequencialmente e conter termo de encerramento com o número total de páginas.

10.6. A licitante deverá enviar a proposta digitalizada, devidamente assinada pelo representante da empresa e as planilhas em meio editável (excel), para fins de conferência.

10.7. O Pregoeiro poderá, justificadamente, sanar erros ou falhas que não alterem a substância das Propostas, atribuindo-lhes validade e eficácia para fins de classificação.

10.8. Todas as especificações do objeto contidas na proposta vinculam a licitante.

11. DOS DOCUMENTOS DE HABILITAÇÃO:

11.1. A proponente deverá apresentar os seguintes documentos de habilitação, caso não conste do SICAF, dele conste vencida, ou não opte por sua habilitação pelo Cadastro:

11.1.1. Habilitação Jurídica:

I. Documento de Identificação contendo todos os dados dos responsáveis legais da proponente.

II. No caso de empresário individual: Inscrição no Registro Público de Empresas Mercantis na Junta Comercial da respectiva sede.

III. No caso de sociedade empresária ou empresa individual de responsabilidade limitada – EIRELI: Ato constitutivo, Estatuto ou Contrato Social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documentos de eleição de seus administradores devidamente publicados e acompanhados de todas as alterações **ou** da consolidação respectiva.

IV. No caso de sociedade simples: Inscrição do Ato Constitutivo no Registro Civil das Pessoas Jurídicas do local da sede, acompanhada de prova da indicação dos seus administradores.

V. No caso de microempresa (ME) ou empresa de pequeno porte (EPP): Certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de ME/EPP. Caso julgue necessário, o Pregoeiro Oficial poderá solicitar a Demonstração do Resultado do Exercício – DRE para fins de aferição da Receita Bruta.

VI. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização.

VII. Procuração por instrumento público, comprovando a delegação de poderes para assinatura e rubrica dos documentos integrantes da habilitação e propostas, quando estas não forem assinadas por diretor(es), com poderes estatutários para firmar compromisso.

11.1.2. Qualificação Técnica: 1 (um) ou mais atestado(s) e/ou declaração(ões) de capacidade técnica, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, em nome da licitante, que comprove(m) a aptidão para desempenho de atividade pertinente e compatível em características e quantidades com o objeto desta licitação.

11.1.2.1. Serão considerados compatíveis os atestados que digam respeito a fornecimento de appliances de firewall em qualquer quantidade, acompanhados do respectivo software de gerência.

11.1.2.2. Os atestados ou certidões deverão ser fornecidos pelos respectivos proprietários dos serviços e deverão conter:

1. Nome, CNPJ, endereço e o telefone da(s) entidade(s) atestante(s);

2. Nome, cargo/função, endereço, telefone e e-mail do(s) representante(s) da(s) sociedade(s) atestante(s) que vier(em) a assinar o(s) atestado(s), a fim de que a VALEC possa com ele(s) manter contato;
3. Nome e CNPJ da sociedade contratada pela(s) sociedade(s) atestante(s) para a execução do objeto atestado;
4. Descrição detalhada do objeto atestado, contendo dados que permitam a aferição de sua similaridade com o objeto licitado;
5. Período e local de execução do objeto;
6. Data da emissão do atestado; e
7. Assinatura do(s) representante(s) da(s) sociedade(s) atestante(s).

11.1.2.3. As informações mínimas que não estejam expressamente indicadas no atestado apresentado pelo Licitante deverão ser comprovadas por meio de documentação complementar anexada ao atestado.

11.1.2.4. A Licitante deve disponibilizar todas as informações necessárias à comprovação da legitimidade dos atestados solicitados, apresentando, quando solicitado, dentre outros documentos, cópia do contrato que deu suporte à contratação, Notas Fiscais/Faturas, Notas de Empenho, e local em que foram prestados os serviços, sendo que estas e outras informações complementares poderão ser requeridas mediante diligência.

11.1.2.5. Os atestados de capacidade técnico-operacional deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificadas no contrato social vigente.

11.1.2.6. Poderão ser apresentados atestados oriundos de contratos distintos, desde que o somatório deles atenda totalmente cada um dos requisitos exigidos.

11.1.3. Qualificação Econômico-Financeira:

I. Certidão negativa de falência, recuperação judicial ou concordata, expedida pelo distribuidor da sede da pessoa jurídica, ou de execução patrimonial, expedida no domicílio da pessoa física (artigo 31 da Lei nº 8.666/93) em data não superior a 120 (cento e vinte) dias.

II. Balanço Patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta.

a) O Balanço Patrimonial e Demonstrações Contábeis, quando se tratar de Sociedade Anônima, deverão ser apresentados na forma de publicação em órgão da imprensa público ou privado de acordo com a legislação vigente.

b) O Balanço Patrimonial e as demonstrações contábeis deverão estar registrados na Junta Comercial ou órgão equivalente, devidamente assinados pelo representante legal da empresa e do contador responsável, (art. 19, § 2º da IN nº 02/2010-MPOG);

12.1.3.1 Com base nos dados extraídos do balanço será avaliada a capacidade financeira da empresa, em conformidade com o art. 19, Inciso XXIV da Instrução Normativa nº 06/2013- MPOG, da seguinte forma:

a) Por meio de **Índices de Liquidez** Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), que deverão ser maiores ou iguais a 1 (um), resultantes da aplicação das fórmulas abaixo, com os valores extraídos de seu balanço patrimonial ou do SICAF:

$$LG = \frac{\text{Ativo Circulante + Realizável a Longo Prazo}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$SG = \frac{\text{Ativo Total}}{\text{Passivo Circulante + Passivo Não Circulante}}$$

$$LC = \frac{\text{Ativo Circulante}}{\text{Passivo Circulante}}$$

b) Cumulativamente, no caso de índices inferiores a 1 (um), proponente deverá comprovar possuir **capital social ou comprovação de patrimônio líquido de 10% (dez por cento)** do valor estimado da contratação.

12.1.3.2 O licitante enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123/2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal e da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

11.1.4 Regularidade Fiscal e Trabalhista:

I. Regularidade Fiscal Federal:

a) Prova de inscrição no Cadastro Nacional de Pessoa Jurídica;

b) Prova de Regularidade com a Fazenda Federal mediante Certidão Conjunta relativa aos tributos federais e à Dívida Ativa da União emitida pela Receita Federal do Brasil – RFB/PGFN;

c) Certificado de Regularidade do Fundo de Garantia do Tempo de Serviço – FGTS;

d) Certificado de Regularidade relativa ao Instituto Nacional do Seguro Social – INSS;

II. Regularidade Fiscal Estadual/Municipal:

a) Prova de inscrição no Cadastro Municipal de Contribuintes, relativo ao domicílio ou sede da proponente, pertinente ao seu ramo de atividade e compatível com o objeto da licitação;

b) Receita Estadual/Distrital

c) Receita Municipal

III. Regularidade Trabalhista: Prova da Regularidade Trabalhista por meio de Certidão emitida pelo Tribunal Superior do Trabalho, conforme o art. 27, inciso IV da Lei 8.666/93.

IV. Declarações constantes do Sistema Comprasnet: deverão ser preenchidas todas as declarações constantes do sistema que serão impressas pelo Pregoeiro.

11.2. Todos os documentos apresentados para habilitação deverão ser apresentados em nome da licitante, com número do CNPJ e com o endereço respectivo.

a) Se a licitante for a matriz, todos os documentos deverão estar em seu nome;

b) Se a licitante for a filial, todos os documentos deverão estar em nome desta, exceto àqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz, e os atestados de capacidade técnica, que podem ser apresentados em nome e CNPJ da matriz e/ou em nome e com o CNPJ da filial.

11.3. Caso a licitante opte por não realizar sua consulta por meio do Sistema SICAF, fica obrigada a apresentar todos os documentos que constem originalmente na consulta de habilitação parcial do SICAF, acima listados.

11.4. As certidões que não apresentarem em seu teor, data de validade previamente estabelecida pelo órgão expedidor, deverão ter sido expedidas até 120 (cento e vinte) dias antes da data da abertura das propostas.

11.5. Será INABILITADO SUMARIAMENTE o licitante que:

a) Enviar a documentação por meio divergente do solicitado pelo Pregoeiro;

b) Enviar documentação incompleta em desacordo com o Edital;

c) Não enviar a documentação pela ferramenta “Convocar Anexo” no prazo estabelecido pelo Pregoeiro;

d) Não enviar a documentação original no prazo estabelecido pelo Pregoeiro;

e) Enviar documentação original divergente daquela disponibilizada no Sistema Comprasnet;

11.6. Após a realização da habilitação no Sistema Comprasnet, o licitante deverá encaminhar toda a documentação original ou em cópia autenticada para a Superintendência de Licitações de Contratos, no escritório da VALEC em Brasília situado no SAUS, Quadra 01, Bloco 'G', Lotes 3 e 5, 12º andar, Asa Sul, CEP: 70.070-010, Brasília/DF , no prazo máximo de 3 (três) dias úteis, contados a partir da Habilitação da Licitante.

12. DOS RECURSOS:

12.1. Existindo intenção de interpor recurso, a licitante deverá manifestá-la **motivadamente**, ao Pregoeiro imediatamente após a divulgação da vencedora, **exclusivamente por meio eletrônico**, em formulário próprio, explicitando sucintamente suas razões.

12.2. Sendo aceita a intenção de recurso, será concedido prazo improrrogável de 3 (três) dias úteis para apresentação de suas razões, que deverá ser enviada **exclusivamente** pelo sistema Comprasnet.

12.3. Não serão aceitas intenções de recurso com motivação imprecisa, genérica, vaga, infundada, sem indicação mínima de qual item do edital foi descumprido.

12.4. Não serão aceitas razões de recurso em desacordo com a motivação expressa na intenção.

12.5. Os demais licitantes, que tiverem interesse, ficarão desde logo notificados a apresentarem contrarrazões, exclusivamente pelo sistema Comprasnet, no mesmo prazo improrrogável de 3 (três) dias úteis, a contar do término do prazo da recorrente, sendo-lhes assegurada vista imediata dos autos, no local indicado no Edital.

13. DA ADJUDICAÇÃO E HOMOLOGAÇÃO:

13.1. O objeto da licitação será adjudicado ao Licitante declarado vencedor, por ato do Pregoeiro, caso não haja interposição de recurso, ou pela autoridade competente, após a regular decisão dos recursos apresentados.

13.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

14. DA ATA DE REGISTRO DE PREÇOS:

14.1. Após a homologação do resultado da licitação será celebrada a respectiva Ata de Registro de Preços, com efeito de compromisso de fornecimento para futura contratação, entre a VALEC e a Licitante Vencedora, e, se for o caso, com os demais classificados que aceitarem fornecer pelo preço do primeiro colocado, obedecida a ordem de classificação e os quantitativos propostos para a formação de cadastro reserva, no caso de exclusão do primeiro colocado da Ata, nas hipóteses previstas nos artigos 20 e 21 do Decreto 7.892/2013.

14.2. A VALEC convocará formalmente o primeiro colocado e demais fornecedores interessados no cadastro reserva para a assinatura da Ata de Registro de Preços, que deverão comparecer no prazo de 10 (dez) dias, contados a partir da data de sua convocação, sob pena de decair do direito à contratação sem prejuízo das sanções previstas no Edital.

14.3. O prazo estabelecido no subitem anterior para assinatura da Ata de Registro de Preços poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo(s) licitante(s) vencedor(s), durante o seu transcurso, e desde que devidamente aceito pela administração.

14.4. Serão formalizadas tantas Atas de Registro de Preços quanto necessárias para o registro de todos os itens e grupos constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

14.5. Na hipótese do não atendimento à convocação para assinatura da Ata de Registro de Preços, de recusa em fazê-lo, ou quando o proponente não apresentar situação regular no ato da assinatura da Ata de Registro de Preços, a VALEC, desde que haja conveniência, procederá a adjudicação à licitante que obtiver a melhor classificação, pela ordem do certame, sem prejuízo da aplicação das penalidades previstas no Termo de Referência, na Lei nº 8.666/93 e na Lei nº 10.520/2005.

14.6. Conforme estabelecido nos itens 1.10.4. a 1.10.8. do Termo de Referência, será permitida a adesão de órgãos não participantes (caronas), desde que observados os limites estabelecidos no Decreto nº 7.892/2013.

15. DA CONVOCAÇÃO DA LICITANTE VENCEDORA:

15.1. Os proponentes serão convocados para assinatura do respectivo instrumento de Contrato, por ordem de classificação, no prazo de 5 (cinco) dias úteis, a contar do recebimento da expressa convocação, podendo ser realizada simultaneamente à da assinatura da Ata de Registro.

15.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte, durante o seu transcurso, e desde que ocorra motivo justificado e aceito pela VALEC.

15.3. Na hipótese de que a Licitante vendedora não compareça ou recuse-se, de maneira injustificada, a cumprir com o objeto ora contratado, fica facultado à VALEC convocar os Licitantes remanescentes, por ordem de classificação, sem prejuízo da aplicação das sanções previstas neste Edital.

16. DAS CONDIÇÕES DA CONTRATAÇÃO

16.1. Nas contratações de serviços comuns com obrigações futuras, deverão ser observadas as demais condições de contratação constantes do Termo de Referência ou Minuta de Contrato Padrão, conforme abaixo indicado:

16.1.1. DAS OBRIGAÇÕES DO FORNECEDOR: Deverão ser observadas as exigências contidas no item 8. do Termo de Referência.

16.1.2. DAS OBRIGAÇÕES DA VALEC: Deverão ser observadas as exigências contidas no item 8.2. do Termo de Referência.

16.1.3. DO CRITÉRIO DE MEDIÇÃO E PAGAMENTO: Deverão ser observadas as exigências contidas item 4. do Termo de Referência**.**

16.1.4. DA GESTÃO E FISCALIZAÇÃO: Deverão ser observadas as exigências contidas no item 5.4 do Termo de Referência.

16.1.5. DAS SANÇÕES E MULTAS: Deverão ser observadas as exigências contidas nos itens 9. E 13. do Termo de Referência.

16.1.6. DA GARANTIA DO OBJETO: Deverão ser observadas as exigências contidas nos itens 19.2. e 24.2. do Termo de Referência.

16.1.7. DA GARANTIA CONTRATUAL: Deverão ser observadas as exigências contidas no item 7. do Termo de Referência.

16.1.8. DA RESCISÃO: Deverão ser observadas as exigências contidas na cláusula décima quarta do Contrato.

16.1.9. DO RECEBIMENTO DO OBJETO: Deverão ser observadas as exigências contidas no item 5.1. a 5.3. do Termo **de** Referência.

16.1.10. DA CESSÃO E SUB-ROGAÇÃO: Deverão ser observadas as exigências contidas item xx do Termo de Referência.

16.1.11. SUBCONTRATAÇÃO: Será permitida a subcontratação parcial dos serviços conforme indicado no item 16. do Termo de Referência.

17. DAS SANÇÕES EDITALÍCIAS:

17.1. Poderá ficar impedido de licitar e contratar com a União, Estados, Distrito Federal ou Municípios, pelo prazo de até 5 (cinco) anos, sem prejuízo da multa de até 10% (dez por cento) do valor do orçamento, bem como das demais cominações legais, o licitante que:

a) Não assinar a Ata de Registro de Preços no prazo estabelecido;

b) Convocado dentro do prazo de validade da sua proposta não celebrar o contrato;

c) Deixar de entregar a documentação exigida para o certame ou apresentar documento falso;

d) Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

e) Não mantiver a proposta, salvo se em decorrência de fato superveniente, devidamente justificado;

f) Fraudar a licitação ou praticar atos fraudulentos na execução do contrato;

g) Comportar-se de modo inidôneo ou cometer fraude fiscal; ou

h) Der causa à inexecução total ou parcial do contrato.

17.2. A aplicação da sanção de impedimento de licitar e contratar implicará no descredenciamento do licitante, pelo prazo de até 5 (cinco) anos do SICAF.

17.3. Aplicam-se as sanções administrativas, criminais e regras gerais previstas no Capítulo IV da Lei nº 8.666/93.

17.4. O Licitante que se declarar como ME/EPP para obtenção dos benefícios da Lei Complementar nº 123/2006 e não possuir tal condição ficará sujeito às sanções administrativas previstas no artigo 7º da Lei nº 10.520/02.

17.5. Da intimação ou da lavratura da Ata de Aplicação de Penas de advertência, multa, suspensão temporária de participação em licitação, impedimento de contratar com a administração pública e declaração de inidoneidade, caberá recurso no prazo de 5 (cinco) dias úteis.

17.6. As penalidades serão obrigatoriamente registradas no SICAF.

17.7. É competência do Pregoeiro propor à autoridade competente a aplicação de sanções ocorridas durante o procedimento licitatório.

17.8. Nos casos de emissão de declaração falsa, a empresa licitante estará sujeita à tipificação no crime de falsidade ideológica, prevista no artigo 299 do Código Penal Brasileiro, bem como nos crimes previstos nos artigos 90 e 93 da Lei nº 8.666/93, além de poder ser punido administrativamente, conforme as sanções previstas no presente Edital.

18. DAS DISPOSIÇÕES GERAIS:

18.1. Os horários estabelecidos no Edital, no aviso e durante a sessão pública observarão, para todos os efeitos, o horário de Brasília, Distrito Federal, inclusive para contagem de tempo e registro no sistema eletrônico e na documentação relativa ao certame, conforme estabelecido o § 5º, do artigo 17 do Decreto nº 5.450/2005.

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

18.3. As normas que disciplinam este Pregão serão sempre interpretadas em favor da ampliação da disputa entre as interessadas, desde que não comprometam o interesse da Administração, a finalidade e a segurança da contratação.

18.4. A presente licitação poderá ser revogada por razões de interesse público decorrente de fato superveniente devidamente comprovado, pertinente e suficiente para justificar sua revogação, devendo ser anulada por ilegalidade, de ofício ou por provocação de terceiros, mediante parecer escrito devidamente fundamentado, assegurado o contraditório e a ampla defesa.

18.5. O presente Edital e suas exigências técnicas foram elaborados em conformidade com a documentação constante na fase interna do processo administrativo acima referenciado, encaminhado pela Superintendência de Tecnologia da Informação e aprovado pela Diretoria de Planejamento, sendo de sua inteira responsabilidade as informações e exigências técnicas contidas no Edital e no Termo de Referência.

ANEXO 1

TERMO DE REFERÊNCIA

1. JUSTIFICATIVA

1.1 OBJETO DA CONTRATAÇÃO

1.1.1 Registro de Preços para eventual Aquisição de Plataforma de Segurança com funcionalidade de proteção à rede, usuários/servidores críticos e inteligência no combate a ameaças, incluindo o fornecimento de equipamentos e softwares integrados em forma de *appliance* e/ou software *appliance* (módulo virtual) quando especificado, serviços de instalação e configuração, suporte técnico e garantia e transferência de conhecimento, conforme especificações constantes neste Termo de Referência.

1.2. QUANTITATIVOS

LOTE 1 – SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO FÍSICO				
ITEM	**DESCRITIVO**	**REQUISIÇÃO INICIAL VALEC**	**REQUISIÇÃO INICIAL DNIT**	**REQUISIÇÃO INICIAL TOTAL**
1	MÓDULO DE CONTROLE DE PERÍMETRO FÍSICO	2	2	**4**
2	MÓDULO DE PROTEÇÃO À USUÁRIOS E SERVIDORES CRÍTICOS	1.200	5000	**6200**
3	MÓDULO DE INTELIGÊNCIA NO COMBATE À AMEAÇAS	1	1	**2**
4	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO DE PERÍMETRO FÍSICO	1	1	**2**
LOTE 2 – SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO VIRTUAL				
ITEM	**DESCRITIVO**	**REQUISIÇÃO INICIAL VALEC**	**REQUISIÇÃO INICIAL DNIT**	**REQUISIÇÃO INICIAL TOTAL**
5	MÓDULO DE CONTROLE DE PERÍMETRO VIRTUAL	4	0	**4**
6	MÓDULO DE GERÊNCIA CENTRALIZADO	1	0	**1**
7	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO E GERÊNCIA CENTRALIZADA DO PERIMETRO VIRTUAL	1	0	**1**

1.2.1. Os itens constantes na planilha de quantitativos foram agrupados em dois lotes afim de garantir maior competitividade e isonomia neste processo, por entendemos que os produtos a serem adquiridos podem ser fornecidos por entidades diferentes sem prejuízo ao objeto pretendido no referido certame.

1.2.2. A contratação de sistema informatizado e dos correspondentes serviços continuados de manutenção pós-garantia devem ser licitados ou adjudicados de forma separada, sempre que esse parcelamento for viável técnica e economicamente e os dois objetos admitirem

fornecedores distintos, nos termos do art. 23, §1º, da Lei 8.666/1993. (Acórdão 1491/2009 Plenário (Sumário))

1.2.3. Em consonância com o disposto nos arts. 3º, § 1º, inciso I, e 23, §§ 1º e 2º, da Lei nº 8.666/1993, incumbe ao gestor promover o parcelamento do objeto a ser licitado com vistas ao melhor aproveitamento dos recursos disponíveis no mercado e à ampliação da competitividade, ou, na impossibilidade técnica e econômica de fazê-lo, apresentar justificativas fundamentadas nos autos do procedimento licitatório. (Acórdão 839/2009 Plenário (Sumário))

1.3. OBJETIVO

1.3.1. Garantir a disponibilidade dos serviços de TI através da aquisição de solução de segurança para prevenção de ataques; evitar que usuários não autorizados acessem serviços ou sistemas; e controlar as ações realizadas na rede da VALEC. Prover linha de redundância para os *enlaces* do Backbone principal.

1.4. MOTIVAÇÃO

1.4.1. Os equipamentos tipo *Firewall* consiste de um dispositivo de rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede. Sua função consiste em regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra (invasão), protegendo assim os recursos de hardware e software.

1.4.2. Este equipamento controla todas as comunicações que passam de uma rede a outra e, em função do que sejam, permite ou denega seu passo. Para permitir ou denegar uma comunicação, o firewall examina o tipo de serviço ao qual corresponde, que podem ser a sites do tipo Portais (Terra, UOL, IG, etc...), correio eletrônico dentre outros.

1.4.3. O firewall também é um grande aliado no combate a vírus e *malwares*, no que tange o uso e bloqueio portas que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados que se utilizam de IP/Porta. Em redes corporativas, como a VALEC, torna-se possível evitar que os usuários acessem serviços ou sistemas indevidos, além de ter o controle sobre as ações realizadas na rede, sendo possível até mesmo rastrear e descobrir quais usuários as efetuaram.

1.4.4. Esse dispositivo de segurança existe na forma de *software* e de *hardware*, a combinação de ambos normalmente é chamado de *appliance*. A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.

1.4.5. Em 2012, a VALEC realizou a aquisição de produtos de Firewall Check Point através da adesão à Ata de Registro de Preços do Tribunal Superior Eleitoral nº 047/2011, decorrente do Edital TSE nº 99/2011, processo nº 16.327/2011 para a Justiça Eleitoral. Todos os equipamentos estão hoje em produção, com capacidade de processamento inferior ao necessário, sem garantia, manutenção e com suporte inválido, sendo que tais serviços encontram-se vencidos.

1.4.6. Através do presente Termo de Referência, pretende-se substituir a plataforma que se encontra defasada diante das necessidades da VALEC. De forma mais detalhada, hoje, a VALEC possui um Check Point Account ID de nº 006807373 onde todos os produtos e licenças adquiridos estão relacionados, conforme quadro abaixo:

Partnumber	Nome do Produto	Descrição	Account ID	Hardware Serial
CPAP-SG4807	4807- Security Gateway Appliance	Check Point 4800 Appliance with FW, VPN, IA, ADNC, MOB, IPS and APCL	6808373	1135C00711

Partnumber	Nome do Produto	Descrição	Account ID	Hardware Serial
CPAP-SG4807-HÁ	4807 HÁ-Security Gateway Appliance	Check Point 4800 Appliance with FW, VPN, IA, ADNC, MOB, IPS and APCL for High Availability	6808373	1135C00685
CPSM-C1000	Security Management Container (10 GW)	Check Point Security Management container to manage up to 10 gateways and 1000 endpoints	6808373	
CPSM-P1007	Security Management for 10 Gateways and 7 Blades	Security Management pre-defined system including container for 10 gateways with 7 Management blades (NPM, EPM, LOGS, MNTR, EVIN, PR)	6808373	

1.4.7. Devido a estrutura da VALEC, é impreterível que a plataforma siga o mesmo modelo adotado na atual estrutura, viabilizando a configuração de Cluster (02 equipamentos em funcionamentos simultâneos do tipo ativo-ativo ou ativo-passivo) de forma a contingenciar a funcionalidade dos equipamentos em caso de falha de um deles, não interrompendo a comunicação das redes, das aplicações e a VPN (Virtual Private Network) que se encontram operacionais entre a VALEC em Brasília e os usuários das unidades descentralizadas.

1.4.8. A utilização da VPN permite a comunicação através de túneis de comunicação criptografados utilizando a Internet pública como meio de comunicação seguro. A adoção deste caminho alternativo de comunicação, ao longo dos últimos três anos de funcionamento, demonstrou ser esta a única alternativa viável para estabelecer a contingência de comunicação entre os usuários da Rede Corporativa da VALEC de maneira mais econômica.

1.4.9. Outra utilização prática dos equipamentos de FIREWALL é o chaveamento (troca) automático entre as linhas de comunicação quando ocorre alguma falha, procedimento que passa despercebido pelos usuários e, também, não há indisponibilidade dos serviços fornecidos.

1.4.10. A cada mês constatamos um aumento da utilização desses links tornando necessária a utilização da alta disponibilidade destes equipamentos, uma vez que atualmente existe apenas um único Firewall/VPN desempenhando esta função, tornando-se este um ponto de falha sensível que precisa ser mitigado.

1.4.11. O concentrador VPN também será atualizado permitindo o aumento da capacidade conexão e aumento do tráfego de informações criptografadas.

1.5. FUNDAMENTAÇÃO LEGAL DA AQUISIÇÃO

1.5.1. Este Termo de Referência foi elaborado à luz dos dispositivos legais, a saber:

1.5.1.1. Decreto nº 7.174/2010 – Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;

1.5.1.2. Decreto nº 6.204 de 05 de setembro de 2007 – Regulamenta o tratamento favorecido, diferenciado e simplificado para as microempresas e empresas de pequeno porte nas contratações públicas de bens, serviços e obras, no âmbito da administração pública federal;

1.5.1.3. Decreto-lei nº 200/1967, art. 10, § 7º - Dispõe sobre a organização da

Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências;

1.5.1.4. Lei Complementar nº 123, de 14 de dezembro de 2006, que institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte;

1.5.1.5. Lei nº 8.666/1993 – Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

1.5.1.6. Lei nº 10.520/2002 – Institui, no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI, da Constituição Federal, modalidade de licitação denominada pregão, para aquisição de bens e serviços comuns, e dá outras providências;

1.5.1.7. Instrução Normativa SLTI nº 04/2014 – Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP) do Poder Executivo Federal. Essa norma aplica-se subsidiariamente à IN/SLTI nº 02/2008;

1.5.1.8. Nota Técnica nº 01/2008 – SEFTI/TCU – Estabelece o conteúdo mínimo do projeto básico ou Termo de Referência para contratação de serviços de Tecnologia da Informação e Comunicações – TIC;

1.5.1.9. Nota Técnica nº 02/2008 – SEFTI/TCU – Estabelece o uso do pregão para aquisição de bens e serviços de Tecnologia da Informação; e

1.5.1.10. Decreto nº 3.931, de 19 de setembro de 2001 e Decreto nº 7.892 de 23 de janeiro de 2013, que regulamentam o sistema de registro de preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993.

1.5.1.11. Decreto nº 7.892, de 23 de janeiro de 2013 – Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei no. 8.666, de 21 de junho de 1993.

1.5.1.12. Decreto nº 8184, de 17 de janeiro de 2014 – Estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de sistemas de tecnologia da informação e comunicação, para fins do disposto no art. 3º da lei nº 8.666, de 21 de junho de 1993;

1.5.1.13. A presente contratação se trata de bem comum, conforme disposto no Art. 1º, da Lei 10.520/02, visto que os padrões de desempenho e qualidade podem ser objetivamente definidos. Assim tendo por base a natureza dos objetos descritos neste instrumento e as demais normas sugere-se a adoção da modalidade Pregão;

1.5.1.14. Pela inconstância orçamentária que vem passando o governo federal, e consequentemente a VALEC, entendemos que poderemos adquirir os produtos constantes nos lotes e itens desse termo de referência de forma parcelada, afim de alinhar a previsão de entregas com o planejamento orçamentário e pagamento dos produtos adquiridos. Dessa forma, sugerimos a formalização por ata de registro de preços, afim garantimos o preço do futuro certame, bem como o ganho em escala, pela volumetria solicitada, bem como a solicitação tardia por outros Órgãos da Administração Pública Federal.

1.6. BENEFÍCIOS E RESULTADOS DA CONTRATAÇÃO

1.6.1. Aumentar a capacidade de tratamento de tráfego;

1.6.2. Impedir que a rede da VALEC seja acessada sem autorização;

1.6.3. Evitar que informações sejam capturadas ou que sistemas tenham seu funcionamento prejudicado pela ação de hackers;

1.6.4. Bloquear “portas” que eventualmente sejam usadas pelas "pragas digitais" ou então bloquear acesso a programas não autorizados na rede da VALEC;

1.6.5. Impedir que ataques de negação de serviços distribuídos indisponibilizem o acesso aos Serviços da VALEC na internet.

1.7. PRAZO PARA EXECUÇÃO

1.7.1. Os itens 1, 2, 3, 5 e 6 deverão ser solicitados por meio de Ordem de Serviços cuja execução deve ser feita em até 60 (sessenta) dias.

1.7.2. Os item 4 e 7 referem-se a prestação de serviço técnico que deverá ser feito imediatamente após abertura da Ordem de Serviço específica para esses itens.

1.8. CARACTERIZAÇÃO DO SERVIÇO – COMUM OU NÃO

1.8.1. O objeto a ser licitado pode ser classificado como comum, sendo amplamente utilizados no mercado de segurança da informação e possuindo diversos fornecedores no Brasil.

1.8.2. Em relação aos itens 4 e 7 informamos que são de natureza continuada por tratar-se de suporte a tecnologia ofertada, apresentando elevado risco ao ambiente tecnológico caso seus serviços sejam descontinuados.

1.9. DEFINIÇÃO PELA APLICAÇÃO OU NÃO DO DIREITO DE PREFERÊNCIA

1.9.1. As regras para aplicação do direito de preferência deverão seguir o que consta no Decreto nº 7174/2010.

1.10. MODALIDADE E TIPOS DE LICITAÇÃO

1.10.1. O planejamento desta licitação foi elaborado de acordo com o Ordenamento Jurídico concernente aos processos de aquisições para a Administração Pública: Lei Complementar nº 123/2006; Lei nº 10.520/2002; Decreto nº 7.892/2013; Decreto nº 7.174/2010; Decreto nº 5.450/2005; IN SLTI/MP nº 04/2014; Nota Técnica nº 01/2008 - SEFTI/TCU; Nota Técnica SEFTI/TCU nº 02/2008; Nota Técnica SEFTI/TCU n° 03/2009; Nota Técnica SEFTI/TCU n° 04/2009; Nota Técnica SEFTI/TCU n° 06/2009 e, subsidiariamente, a Lei nº 8.666/93 e a IN SLTI/MP nº 02/2008, sendo os respectivos artefatos indispensáveis e inseparáveis do processo licitatório.

1.10.2. Desse modo, o presente documento contém os elementos básicos e essenciais determinados pela legislação, descritos de forma a subsidiar os interessados em participarem do certame licitatório na preparação da documentação e na elaboração da proposta.

1.10.3. Em conformidade com o exposto no bojo dos estudos realizados anteriormente, entende-se que o certame deverá ser processado pela modalidade Pregão, a ser realizado de forma eletrônica, com vistas a obter a melhor proposta para a Administração Pública.

1.10.4. Será admitida adesões nos lotes à Ata de Registro de Preços – ARP gerada a partir deste SRP, que deverão seguir o disposto no Decreto nº 7.892/2013.

1.10.5. As aquisições ou contratações adicionais, em atendimento ao art. 22, § 3º, do Decreto nº 7.892/2013, não poderão exceder, por órgão ou entidade, a cem por cento dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

1.10.6. O quantitativo decorrente das adesões à Ata de Registro de Preços por órgãos ou entidades não participantes (adesões tardias) não poderá exceder, na totalidade, os limites estabelecidos no art. 22, § 4º, do Decreto nº 7.892/2013, independentemente do número de órgãos não participantes que aderirem, isto é, não poderá exceder, na totalidade, ao quíntuplo do quantitativo de cada item registrado na ata de registro de preços para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

1.10.7. A Ata de Registro de Preços terá validade de 12 (meses) ano contado a partir da data de sua assinatura.

1.10.8. Durante sua vigência, a Ata de Registro de Preços poderá ser utilizada por qualquer órgão ou entidade da Administração Pública que não tenha participado deste

Pregão (carona tardia), mediante prévia consulta ao Gestor da VALEC, desde que devidamente comprovada a vantagem, não podendo exceder, por órgão ou entidade, a 100% (cem por cento) dos quantitativos registrados, podendo-se replicar 5 vezes.

1.11. Deveres e Responsabilidades do Órgão Gerenciador do Registro de Preços

1.11.1. Efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços.

1.11.2. Conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;

1.11.3. Aplicar as penalidades por descumprimento do pactuado na Ata de Registro de Preços.

1.11.4. Autorizar ou não o fornecimento da Solução de Tecnologia da Informação para órgão não participante da Ata de Registro de Preços, desde que prevista no instrumento convocatório, consultando o beneficiário da Ata e verificando as condições de fornecimento, de forma a evitar extrapolações dos limites de produtividade ou de capacidade mínima de fornecimento da Solução.

1.11.5. Definir mecanismos de comunicação com os órgãos participantes, não participantes, contendo:

1.11.5.1.1. As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível.

1.11.5.1.2. Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável, a exemplo de ordem de serviço ou fornecimento de bens, aplicação de sanções administrativas, alteração de item registrado em Ata por modelo equivalente ou superior.

1.11.6. Definir mecanismos de controle de fornecimento da Solução de Tecnologia da Informação, observando, entre outros:

1.11.6.1. A definição da produtividade ou da capacidade mínima de fornecimento da Solução de Tecnologia da Informação.

1.11.6.2. Regras para fornecimento da Solução de Tecnologia da Informação aos órgãos não participantes, desde que previsto no instrumento convocatório, cujo fornecimento não poderá prejudicar os compromissos já assumidos e as futuras contratações dos órgãos participantes do registro de preços.

1.11.6.3. Regras para gerenciamento da fila de fornecimento da Solução de Tecnologia da Informação aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pela CONTRATADA.

1.12. CONEXÃO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO EXISTENTE

1.12.1. A contratação dos bens e serviços pretendidos vão ao encontro dos objetivos estratégicos da VALEC no que tange à segurança da informação, conforme necessidade 34 – Contratação e Manutenção de solução de segurança da informação.

1.13. **CRITÉRIOS AMBIENTAIS ADOTADOS**

1.13.1. Para esta contratação foram consideradas as circunstâncias sob as quais os produtos gerem mais eficiência à Administração Pública Federal. A escolha não considerou aspectos do que já existe na empresa e com a finalidade de preservar os investimentos já feitos não optou-se pela continuidade dos produtos e serviços, de modo a gerar o menor impacto ambiental e social possível.

2. ESPECIFICAÇÃO TÉCNICA

A Especificação técnica do projeto, encontra-se no Anexo I.

3. MODELO DE PRESTAÇÃO DE SERVIÇO / FORNECIMENTO DE BENS

3.1. ATORES ENVOLVIDOS NO PROCESSO

3.1.1. **Gestor do Contrato** - Servidor com atribuições gerenciais, técnicas e operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente.

3.1.2. **Fiscal Administrativo:** Servidor competente para fiscalizar a parte administrativa do contrato.

3.1.3. **Fiscal Técnico:** Servidor competente para fiscalizar a parte técnica do contrato.

3.1.4. **Fiscal Requisitante:** Servidor competente para fiscalizar a parte funcional do contrato do contrato.

3.1.5. **Preposto** - Funcionário representante da contratada, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto a contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.

3.1.6. A gestão do contrato fica a cargo de servidor da VALEC

3.1.7. Este Termo de Referência deverá ser de total conhecimento do Gestor do Contrato, que deve acompanhar todos os detalhes do processo licitatório, desde o planejamento até a sua execução.

3.1.8. A Administração indicará representantes especialmente designados, nos termos dos Artigos 67 e 73 da Lei Nº 8.666/93 e do Art. 6º do Decreto Nº 2.271/97, para acompanhamento e fiscalização do contrato, nos termos especificados no Edital. A fiscalização será exercida no interesse da Administração e não exclui nem reduz a responsabilidade da Licitante vencedora, inclusive perante terceiros, por quaisquer irregularidades, e, na sua ocorrência, não implica corresponsabilidade do Poder Público ou de seus agentes e prepostos.

3.1.9. Caberá ao servidor indicado rejeitar totalmente ou em parte, quaisquer sistemas que não estejam de acordo com as exigências, ou àqueles que não sejam comprovadamente original ou novo, assim considerado de primeiro uso, podendo ser substituído qualquer equipamento eventualmente fora de especificação.

3.2. PROTOCOLO DE COMUNICAÇÃO ENTRE A CONTRANTANTE E A CONTRATADA

3.1.1. São mecanismos formais de comunicação entre a Contratada e a Contratante:

3.1.2. E-mails: forma rápida de comunicação para tratar de informações pouco críticas;

3.1.3. Ofícios: Comunicação para tratar de assuntos gerais;

3.1.4. Ordem de Serviço: elaborada, por demanda, pela Contratante e encaminhada via sistema eletrônico, correio eletrônico ou ligação telefônica à Contratada, com a função de

demandar serviços contratados;
3.1.5. Termo de Recebimento Provisório: termo elaborado pela Contratante e encaminhado à Contratada.
3.1.6. Termo de Recebimento Definitivo: termo elaborado pela Contratante e encaminhado à Contratada.

4. FORMA DE PAGAMENTO

4.1. Os valores referentes aos serviços devem ser pagos por demanda, de acordo com a emissão de ordem de serviço com o aceite definitivo realizado.
4.2. O pagamento será efetuado à CONTRATADA, no prazo de até 30 (trinta) dias úteis contados da data da emissão da apresentação da fatura ou nota fiscal;
4.3. A Nota Fiscal/Fatura não poderá ser apresentada antes solicitação do gestor, que atestará os serviços;
4.4. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP

Na qual:

I = (TX/100)/365

Onde: EM = Encargos moratórios.

I = Índice de atualização financeira.

TX = Taxa de Juro Anual.

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.

VP = Valor da parcela em atraso; = 0,00016438, assim apurado:

I = (i/100)/365; onde i = taxa percentual anual no valor de 6%;

4.5. No caso de incorreção dos documentos apresentados, inclusive na Nota Fiscal/Fatura, serão os mesmos restituídos à CONTRATADA para correções necessárias, não respondendo a VALEC por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes;
4.6. Caso a contratada seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresa de Pequeno Porte – SIMPLES, deverá apresentar juntamente com a Nota Fiscal/Fatura a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor;
4.7. Constatada a irregularidade fiscal por meio de consulta on-line ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou a documentação mencionada no art. 29 da Lei 8.666/93, a empresa será advertida, por escrito, para que no prazo de até 05 (cinco) dias úteis, apresente a regularização fiscal junto ao SICAF, sob pena de rescisão do contrato; e
4.8. O prazo para regularização poderá ser prorrogado desde que a justificativa apresentada seja aceita pela contratante.

5. MÉTODO DE AVALIAÇÃO DE CONFORMIDADE DOS PRODUTOS E SERVIÇOS

5.1. RECEBIMENTO PROVISÓRIO

5.1.1. O Contratante realizará o recebimento provisório do(s) equipamento(s), do(s) software(s) e serviço(s) no momento da entrega;
5.1.1.1. Todos os equipamentos/serviços deverão ser entregues/prestados em

Brasília, ou em local previamente acordado no reunião de instrução, no horário de funcionamento do Órgão;

5.1.2. A equipe técnica da SUPTI da Valec realizará inspeção técnica dos equipamentos para verificação da sua integridade física e aderência às especificações constantes do Edital;

5.1.3. Após a inspeção técnica nos equipamentos e verificando que estes estão em perfeitas condições, a Equipe Técnica deverá emitir o Termo de Recebimento Provisório, a ser entregue ao Preposto ou Representante da Contratada. Este documento garante à CONTRATADA que os itens constantes da OS foram entregues à CONTRATANTE para avaliação de sua qualidade e conformidade.

5.1.4. Os equipamentos deverão ser entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões e/ou outros problemas físicos;

5.1.5. O(s) equipamento(s), acessório(s) e/ou componente(s) entregue(s) que apresentarem inconformidades, defeito por transporte e/ou por processo fabril, deverá(ão) ser substituído(s) pela Contratada, em um prazo de 15 (quinze) dias corridos, contados a partir da notificação pelo contratante;

5.2. RECEBIMENTO DEFINITIVOS

5.2.1. Verificando-se a conformidade dos itens da OS entregues pela CONTRATADA, a CONTRATANTE deve verificar se a execução da Ordem de Serviço se deu de forma aderente aos termos contratuais. Estando o processo aderente, a CONTRATANTE emitirá o Termo de Recebimento Definitivo, que será entregue à CONTRATADA.

5.2.2. Caso seja verificada a não aderência aos termos contratuais, a CONTRATANTE deverá indicar os termos que não estão aderentes ao Contrato e deverá encaminha à sua Área Administrativa as sanções cabíveis

5.3. ORDEM DE SERVIÇO – MODELO

5.3.1. Conforme Anexo VII.

5.4. FISCALIZAÇÃO DO CONTRATO

5.4.1. Para o acompanhamento e a fiscalização da execução do contrato serão designados representantes da VALEC, nos termos do artigo 67 da Lei nº 8.666/93 e da Instrução Normativa SLTI/MP nº 04/2014, que se responsabilizarão pelo registro de todas as ocorrências relacionadas com a execução e determinarão o que for necessário à regularização de falhas ou defeitos observados.

5.4.2. A fiscalização de que trata o item anterior não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios, e, na ocorrência desta, não implica em corresponsabilidade da VALEC ou de seus agentes, em conformidade com o artigo 70 da Lei nº 8.666/93.

5.4.3. O contrato será acompanhado e fiscalizado pelos seguintes agentes da VALEC:

5.4.3.1. Fiscal Técnico, Fiscal Administrativo, Fiscal Requisitante, Gestor do Contrato.

5.4.4. O contrato será acompanhado por empregados da VALEC, com o objetivo de garantir a adequada prestação dos serviços e o fornecimento dos bens que compõem a Solução de Tecnologia da Informação durante todo o período de sua execução e compreende, nos termos da Instrução Normativa SLTI/MP nº 04/2010, as seguintes tarefas:

5.4.5. Realização de reunião inicial, convocada pelo seu **gestor**, com a participação dos **fiscais**, da Contratada, e demais intervenientes por ele identificados, para apresentação do preposto e dos serviços oferecidos pela Contratada; breve explanação sobre o portal de acesso à sua base de conhecimento; entrega do termo de compromisso e do termo de ciência;

esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do contrato, dentre outros assuntos que forem relevantes para dar início à sua execução;

5.4.6. Encaminhamento formal de Autorização de Início dos Serviços pelo **gestor** do contrato ao preposto da contratada;

5.4.7. Monitoramento da execução, pelos **fiscais** e pelo **gestor** do contrato;

5.4.8. Confecção e assinatura do Termo de Recebimento Provisório, cujo modelo consta do **ANEXO III** deste Termo de Referência, a cargo do **fiscal técnico** do contrato;

5.4.9. Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os critérios de aceitação definidos em contrato, a cargo dos **fiscais técnico** e **requisitante** do contrato;

5.4.10. Identificação de não conformidade com os termos contratuais, a cargo dos **fiscais técnico** e **requisitante** do contrato;

5.4.11. Verificação de aderência aos termos contratuais, a cargo do **fiscal administrativo** do contrato;

5.4.12. Verificação da manutenção das condições classificatórias referentes à habilitação técnica, a cargo dos **fiscais administrativo** e **técnico** do contrato;

5.4.13. Encaminhamento das demandas de correção à Contratada, a cargo do **gestor** do contrato;

5.4.14. Encaminhamento de indicação de sanções por parte do **gestor** do contrato para a Área Administrativa;

5.4.15. Confecção e assinatura do Termo de Recebimento Definitivo, para fins de encaminhamento para pagamento, cujo modelo consta do **ANEXO VI** deste Termo de Referência, a cargo do **gestor** e do **fiscal requisitante** do contrato;

5.4.16. Verificação das regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento, a cargo do **fiscal administrativo** do contrato;

5.4.17. Verificação da manutenção da necessidade, economicidade e oportunidade da contratação, a cargo do **fiscal requisitante** do contrato;

5.4.18. Verificação de manutenção das condições elencadas no Plano de Sustentação, a cargo dos **fiscais técnico e requisitante** do contrato;

5.4.19. Encaminhamento à Área Administrativa de eventuais pedidos de modificação contratual, a cargo do **gestor** do contrato; e

5.4.20. Manutenção do histórico de gerenciamento do contrato, contendo registros formais de todas as ocorrências positivas e negativas da execução do contrato, por ordem histórica, a cargo do **gestor** do contrato;

5.4.21. Transição contratual, quando aplicável, e encerramento do contrato, que deverá observar o Plano de Sustentação; e

5.4.22. No caso de prorrogação contratual, o **gestor** do contrato deverá, com base na documentação contida no histórico de gerenciamento do contrato e nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, encaminhar à Área Administrativa, com pelo menos 60 (sessenta) dias de antecedência do término do contrato, documentação explicitando os motivos para a prorrogação; e

5.4.23. No caso dos demais aditamentos contratuais, o **gestor** do contrato deverá encaminhar, à Área Administrativa, documentação explicitando os motivos para tal aditamento.

5.4.24. A gestão e fiscalização deste contrato pela VALEC não excluem nem reduzem a responsabilidade da Contratada pelo cumprimento das obrigações decorrentes deste instrumento.

5.5. VIGÊNCIA E PRORROGAÇÃO DO CONTRATO

5.5.1. O prazo de vigência dos itens 1, 2, 3, 5 e 6 do objeto da contratação é de 48 (quarenta e oito) meses, contados da data de sua assinatura, podendo ser renovado.

5.5.2. A vigência do contrato para os itens 4 e 7 do objeto da contratação é de

48 (quarenta e oito) meses, contados a partir da data de assinatura, podendo ser renovado por mais 12 (doze) meses. Esses serviços referem-se à prestação de natureza contínua, razão pela qual podem vigorar por esse período, tendo como fundamento o que dispõe o inc. II, art. 57 da Lei 8.666/93.

6. REAJUSTE DE PREÇO

6.1. No que não contrariar o art. 5º do Decreto nº 2.271, de 07 de julho de 1997, a cláusula do contrato que se refere a reajuste, se regerá da seguinte forma:

6.1.1. O preço do contrato é fixo e irreajustável para os itens 1, 2, 3, 5 e 6.

6.1.2. O preço do contrato poderá ser reajustado para os itens 4 e 7, caso haja renovação contratual, após o período de 48 (quarenta e oito) meses.

6.2. Na situação de reajuste, esse deverá ser feito utilizando o IPCA, dos 12 últimos meses contados 2 meses antes do vencimento do contrato, como índice de reajuste, ou outro que venha a substituí-lo, conforme art. 19, XXII, da IN 02/2008, obedecida a legislação vigente.

7. GARANTIA CONTRATUAL

7.1. A CONTRATADA deverá apresentar, no prazo máximo de 10 (dez) dias úteis, prorrogáveis por igual período, a critério do órgão CONTRATANTE, contados da assinatura do Contrato, comprovante de prestação de garantia, sob pena de aplicação de sanções previstas neste Contrato e no Edital;

7.2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

7.3. 1. prejuízos advindos do não cumprimento do objeto do Contrato;

7.4. 2. prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do Contrato;

7.5. 3. multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;

7.6. 4. obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela CONTRATADA, quando couber;

7.7. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados nos itens da alínea "7.2", observada a legislação que rege a matéria;

7.8. A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal em conta específica com correção monetária, em favor do CONTRATANTE;

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

7.10. O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas Cláusulas.

7.11. O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA;

7.12. A garantia será considerada extinta:

7.13. Com a devolução da apólice, fiança bancária 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;

7.14. O prazo de 90 (noventa) dias após o término da vigência do Contrato, que poderá ser estendido em caso de ocorrência de sinistros;

8. DEVERES E RESPONSABILIDADES DA CONTRATADA

8.1.1. Cumprir fielmente as obrigações assumidas em contrato, observando as definições técnicas deste Termo de Referência, entregando os serviços no prazo estipulado, na forma e nas condições pactuadas;
8.1.2. Manter-se, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do mesmo;
8.1.3. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de serviços extras;
8.1.4. Submeter à aprovação da VALEC qualquer alteração que se tornar essencial à continuação da execução ou prestação dos serviços;
8.1.5. Aceitar, nas mesmas condições contratuais, os acréscimos ou as supressões que se fizerem no objeto contratual, até 25% do seu valor inicial;
8.1.6. Refazer os serviços nos quais se verifiquem danos ou qualquer defeito nos materiais e sistemas utilizados, no prazo máximo de 5 (cinco) dias úteis, contados da notificação que lhe for entregue oficialmente, sob pena sofrer sanções por inexecução contratual;
8.1.7. Comunicar à VALEC, por escrito, no prazo máximo de 05 (cinco) dias úteis que antecedem o prazo de vencimento das entregas, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos;
8.1.8. Obter todo e qualquer tipo de licença junto aos órgãos fiscalizadores para o perfeito e efetivo fornecimento da solução ofertada, sem ônus adicional para a VALEC;
8.1.9. Arcar com todas as despesas referentes à prestação dos serviços, tais como frete, seguro, taxas, transportes e embalagens, bem como os encargos trabalhistas, previdenciários, comerciais e salários dos seus empregados, para entrega do serviço no prazo estipulado;
8.1.10. Cumprir com as normas de segurança e medicina do trabalho durante possível estadia dos seus profissionais nas instalações da VALEC;
8.1.11. Assumir todas as responsabilidades e tomar as medidas necessárias ao atendimento dos seus empregados, acidentados ou acometidos de mal súbito, quando em serviço, assegurando-lhes o cumprimento a todas as determinações trabalhistas e previdenciárias cabíveis e assumindo, ainda, as responsabilidades civis, penais, criminais e demais sanções legais decorrentes do eventual descumprimento destas;
8.1.12. Cumprir, além dos postulados legais vigentes de âmbito, federal, estadual, distrital e/ou municipal, as normas de segurança do CONTRATANTE, inclusive quanto à prevenção de incêndios e as de Segurança e Medicina do Trabalho;
8.1.13. Emitir Comunicado de Acidente de Trabalho – CAT, em formulário próprio do INSS, em caso de eventual ocorrência de acidente com seus empregados nas dependências do CONTRATANTE, apresentando cópia do mesmo à Fiscalização do Contrato;
8.1.14. Responder pelos danos, decorrentes de sua culpa ou dolo, causados diretamente à Administração ou a terceiros, não excluindo ou reduzindo esta responsabilidade à Fiscalização e acompanhamento por parte do CONTRATANTE;
8.1.15. Arcar com os prejuízos e danos causados pelos seus funcionários aos bens móveis, imóveis, sistemas, utensílios, mobiliário, etc., da VALEC, substituindo-os após comunicação formal do Fiscal do Contrato, por materiais ou bens idênticos ou recuperados quando possível, deixando-os em perfeito estado de conservação ou funcionamento no prazo máximo de 72 (setenta e duas) horas;
8.1.16. Agendar, pelo telefone (61)2029-6428, a entrada de sistemas ou materiais no ambiente da VALEC, dentro do horário das 09h às 12h e das 14h às 18h, de segunda a sexta-feira, em dias úteis, a fim de que seja designado pessoal técnico da VALEC para a verificação e acompanhamento;

8.1.17. Manter seus funcionários ou representantes credenciados devidamente identificados quando da execução de qualquer serviço nas dependências da VALEC referente ao objeto contratado observando as normas de segurança (interna e de conduta);
8.1.18. Atender às solicitações emitidas pela gestão do contrato quanto ao fornecimento de informações e/ou documentação;
8.1.19. Manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão da execução dos serviços, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros;
8.1.20. Indicar o preposto para, em todas as questões relativas ao cumprimento dos serviços, representar a contratada, de forma a garantir a presteza e a agilidade necessária ao processo decisório. O Preposto será o responsável da contratada pela execução do contrato, e deverá e reportar-se à VALEC, indicando seu cargo, endereço com CEP, número de telefone residencial e celular, número do fac-símile e endereço eletrônico;
8.1.21. Emitir Relatório de Serviços, depois de concluída qualquer manutenção, onde constem informações referentes ao serviço realizado, número do chamado, data e hora do chamado, e hora do início e do término do atendimento;
8.1.22. O relatório deverá ser acompanhado, ainda, de eventual comunicação de novas versões de software, patches de atualização e vulnerabilidades encontradas nos produtos.

8.2. DEVERES E RESPONSABILIDADES DA CONTRATANTE

8.2.1. Prestar informações e esclarecimentos que venham a ser solicitados pela contratada;
8.2.2. Acompanhar e fiscalizar o andamento dos serviços de assistência técnica, devendo para tanto nomear um fiscal de contrato e um gestor, ou uma comissão, que responsabilizar-se-ão pelo acompanhamento dos serviços, conferência e atesto das faturas e cumprimento das demais exigências previstas no contrato;
8.2.3. Observar para que, durante a vigência do contrato, sejam mantidas, pela contratada, as compatibilidades com as obrigações assumidas e todas as condições e qualificações exigidas para a pactuação;
8.2.4. Comunicar formal, circunstanciada e tempestivamente à contratada, qualquer anormalidade ocorrida durante a execução do Contrato;
8.2.5. Promover os pagamentos na forma pactuada;
8.2.6. Receber e atestar as faturas, quando do aceite definitivo, conforme condições e especificações constantes deste Termo de Referência;
8.2.7. Proceder à consulta ao SICAF antes de efetuar o pagamento;
8.2.8. Indicar um técnico para acompanhar a entrega dos produtos;
8.2.9. Permitir acesso dos profissionais da contratada às suas dependências quando da prestação dos serviços;
8.2.10. Receber e conferir a solução entregue, procedendo à imediata devolução daquela que se encontrar com especificação em desacordo do exigido no Contrato;
8.2.11. Solicitar assistência técnica quando da constatação de algum defeito na operacionalização da Solução;
8.2.12. Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando a mesma estiver em conformidade com os padrões de informação e qualidade exigidos;
8.2.13. Exigir, uma vez comprovada a necessidade, o imediato afastamento do ambiente da VALEC, de qualquer profissional e/ou preposto da contratada que, por justas razões, vier a desmerecer a confiança, embarace a fiscalização ou, ainda, que venha a se conduzir de modo inconveniente ou incompatível com o exercício das funções que lhe forem delegadas;

8.2.14. Solicitar ao Gestor do Contrato as decisões e providências que ultrapassem a sua competência, em tempo hábil, para adequada adoção das medidas julgadas cabíveis, quando a contratada não cumprir com as obrigações avençadas.

9. NÍVEIS DE SERVIÇO

9.1. A metodologia de avaliação do nível de serviço será realizada a partir da comparação com um valor de referência mínimo, por meio da mensuração de critérios objetivos e avaliação dos diversos fatores relacionados ao serviço contratado.

9.2. De forma a aferir esse valor mínimo aceitável será utilizado como parâmetro o Índice de Cumprimento de Prazo – ICP. O ICP será aplicado em cada Ordem de Serviço executada pela CONTRATADA, e será calculado através da razão do Prazo Planejado (PP) e do Período da Efetiva Execução (PE), conforme a seguinte fórmula: ICP = PP/PE.

9.3. Esses períodos citados acima são referentes às atividades executadas pela CONTRATADA, que fazem parte do cronograma da OS, e são quantificados em dias úteis. Os prazos para execução são definidos e acordados com a CONTRATADA, atentando-se para os padrões de qualidade exigidos e para as condições contratuais da prestação dos serviços.

9.4. O valor de referência será medido mensalmente e terá como mínimo aceitável o percentual de 0,6. O não atendimento do mínimo aceitável (0,6) ensejará a aplicação das sanções que serão previstas no termo de referência. No caso de serviços entregues antes do prazo estipulado, o ICP terá o valor igual a 1 (um).

9.5. Ademais, para o atendimento a chamados de suporte técnico à Solução deverão ser utilizadas as seguintes definições:

a) Chamados por parada parcial dos módulos e componentes da Solução deverão ser atendidos em até 2 (duas) horas após sua abertura, e poderão incluir um esforço da CONTRATADA com vistas a aplicar as soluções necessárias em até 8 (oito) horas, contadas a partir do início do atendimento;

9.6. Os chamados por parada total dos módulos e componentes da Solução deverão ser atendidos em até 1 (uma) hora após sua abertura, e poderão incluir um esforço da CONTRATADA com vistas a aplicar as soluções necessárias em até 8 (oito) horas, contadas a partir do início do atendimento;

10. DIREITO DE PROPRIEDADE INTELECTUAL

10.1. Pertence à VALEC, nos termos do artigo 111 da Lei nº 8.666/93 c/c a Lei nº 9.609/1998 e a Lei 9.610/1998, o direito patrimonial e a propriedade intelectual dos sistemas mantidos e/ou desenvolvidos e resultados produzidos em consequência desta contratação, entendendo-se por resultados, quaisquer estudos, relatórios, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, fluxogramas, listagens de programas de computador (fonte ou executável) e documentação didática, em papel ou em mídia eletrônica.

10.2. Não será permita a cessão, citação ou qualquer referência pública a nenhum dos trabalhos realizados com a exceção dos autorizados pela VALEC.

10.3. Todos os produtos concebidos durante a execução dos serviços deste Termo de Referência deverão ser rotineiramente sincronizados com o repositório de documentos da VALEC.

10.4. Fica a contratada obrigada a transferir para a VALEC, os direitos patrimoniais de seus empregados sobre os produtos e/ou serviços gerados na execução do objeto desta contratação.

10.5. A contratada responderá por qualquer demanda em relação aos direitos patrimoniais dos seus empregados, não havendo qualquer responsabilidade do contratante e, no caso eventual de imputação de responsabilidade à VALEC na via judicial, a contratada arcará com o pagamento dos valores.

11. SIGILO, RESTRIÇÕES

11.1.1. **Publicidade**

É proibida a publicidade, direta ou indiretamente relacionada com os serviços constantes deste Termo de Referência, salvo se houver autorização por escrito da VALEC.

11.1.2. **Segurança**

Por questões de segurança, fica a contratada obrigada a apresentar todas e quaisquer informações e documentações solicitadas pela VALEC dos profissionais indicados para realizar a manutenção dos sistemas.

11.1.3. **Sigilo**

Será exigida da contratada que assine um termo de compromisso, pelo qual se compromete a mantes o sigilo e a confidencialidade de todas as informações de que venha a ter conhecimento no exercício de suas atribuições, e que a mesma o exija dos seus **empregados que prestarem serviços na VALEC.**

11.1.4. **Idoneidade**

A VALEC se reserva o direito de proceder com levantamento e/ou informações pertinentes à idoneidade de qualquer profissional que venha a ser indicado para a prestação dos serviços.

12. ESTIMATIVA DE PREÇO

12.1. Em consulta ao mercado, foram coletados os preços conforme tabela abaixo:

PROPOSTAS COMERCIAIS FORNECEDORES

LOTE	ITEM	DESCRIÇÃO DOS ITENS	QTD VALEC	QTD DNIT	QTD TOTAL	UNIDADE	VALOR UNITÁRIO	VALOR UNITÁRIO	VALOR UNITÁRIO	VALOR UNITÁRIO	VALOR UNITÁRIO MÉDIO	VALOR MÉDIO TOTAL
1 - Solução de Proteção de Perímetro Físico	1	MÓDULO DE CONTROLE DE PERÍMETRO FÍSICO	2	2	4	HARDWARE	R$ 1.810.000,00	R$ 2.107.043,78	R$ 1.978.534,06	R$ 1.950.000,00	R$ 1.961.394,46	R$ 7.845.577,84
	2	MÓDULO DE PROTEÇÃO À USUÁRIOS E SERVIDORES CRÍTICOS	1200	5000	6.200	LICENÇA	R$ 1.334,00	R$ 1.853,25	R$ 1.517,12	R$ 1.500,00	R$ 1.551,09	R$ 9.616.773,50
	3	MÓDULO DE INTELIGÊNCIA NO COMBATE À AMEAÇAS	1	1	2	LICENÇA	R$ 1.098.000,00	R$ 1.359.560,01	R$ 1.395.231,75	R$ 1.245.000,00	R$ 1.274.447,94	R$ 2.548.895,88
	4	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO DE PERÍMETRO FÍSICO	1	1	2	SERVIÇO	R$ 671.000,00	R$ 780.320,00	R$ 865.375,00	R$ 732.000,00	R$ 762.173,75	R$ 1.524.347,50
2 - Solução de Proteção de Perímetro Virtual	5	MÓDULO DE CONTROLE DE PERÍMETRO VIRTUAL	4	0	4	SOFTWARE	R$ 144.450,00	R$ 212.780,75	R$ 162.196,00	R$ 155.000,00	R$ 168.606,69	R$ 674.426,75
	6	MÓDULO DE GERÊNCIA CENTRALIZADO	1	0	1	SOFWARE	R$ 378.670,00	R$ 435.090,80	R$ 514.280,00	R$ 399.000,00	R$ 431.760,20	R$ 431.760,20
	7	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO E GERÊNCIA CENTRALIZADA DO PERIMETRO VIRTUAL	1	0	1	SERVIÇO	R$ 283.880,00	R$ 396.210,29	R$ 410.435,00	R$ 304.000,00	R$ 348.631,32	R$ 348.631,32
											TOTAL VALOR MÉDIO	**R$ 22.990.412,99**

12.2 Diante dos valores apresentados, entendemos como valor estimado para o projeto em referência, a média aritmética dos valores totais das propostas. Desse o valor estimado para os quantitativos requeridos para a VALEC é de R$ 9.275.539,88 (nove milhões, duzentos e setenta e cinco mil, quinhentos e trinta e nove reais e oitenta e oito centavos), sendo R$ 8.164.734,81 (oito milhões, cento e sessenta e quatro mil, setecentos e trinta e quatro reais e oitenta e um centavos) para aquisição de equipamentos e licenças (investimento) e R$ 1.110.805,07 (um milhão, cento e dez mil, oitocentos e cinco reais e sete centavos) para serviços (custeio).

12.3 Os valores requeridos pelo DNIT são de R$ 13.714.873,11 (treze milhões, setecentos e quatorze mil, oitocentos e setenta e três reais e onze centavos), sendo R$ 12.952.699,36 (doze milhões novecentos e cinquenta e dois mil, seiscentos e noventa e nove reais e trinta e seis centavos) para aquisição de equipamentos e licenças (investimento e R$ 762.173,75 (setecentos e sessenta e dois mil, cento e setenta e três reais e setenta e cinco centavos), para serviços (custeio).

12.4 Diante do exposto, informamos que o total do projeto (VALEC+DNIT) é de R$ 22.990.412,99 (vinte e dois milhões, novecentos e noventa mil, quatrocentos e doze reais e noventa e nove centavos.

13. SANÇÕES APLICÁVEIS

13.1 Pela inexecução total ou parcial das obrigações assumidas, garantidas a prévia defesa, a Administração poderá aplicar à Contratada, as sanções previstas em contrato e neste Termo de Referência, conforme descrição a seguir:

a. Advertência, nos termos da Lei;

b. Multas conforme descrição a seguir:

I. O atraso injustificado no cumprimento dos prazos assumidos em contrato implicará em multa de 0,33 % (trinta e três centésimos por cento) por dia útil após a data fixada, calculada sobre o valor total da fatura a ser paga, até o limite máximo de 10% (dez por cento).

II. Na hipótese mencionada no subitem anterior, a atraso injustificado ou cuja justificativa tenha sido rejeitada pela VALEC, superior a 30 (trinta) dias úteis, caracterizará o descumprimento das obrigações, total ou parcial, conforme o caso, sendo passível de punição com advertência e multa de 20% (vinte por cento) sobre o valor total do contrato, assim como configurada a inexecução do contrato, podendo a VALEC rescindi-lo unilateralmente.

III. A inobservância dos prazos de atendimento dos chamados relativos à Garantia e Assistência, conforme disposto no Acordo de Nível de Serviço constante do subitem 9, implicará à contratada, além das penalidades previstas no Anexo IV, a cominação de rescisão unilateral pela Administração Pública, do contrato firmado, por inexecução contratual.

IV. A rescisão a que se refere a alínea anterior será precedida de punição com multa de 20% (vinte por cento) sobre o valor total do contrato.

V. As multas e glosas porventura aplicadas serão descontadas dos pagamentos devidos pelo contratante, da garantia do contrato, ou cobradas diretamente da contratada, amigável ou judicialmente, e poderão ser aplicadas cumulativamente com as demais sanções previstas.

c. Suspensão temporária de participação em licitações e impedimento de contratar com a União;

d. Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

13.2 Aquele que deixar de entregar os documentos, ou apresentar documentação exigida para o certame, falsa; ensejar o retardamento da execução do objeto contratual; não mantiver a proposta; falhar ou fraudar a execução do contrato; comportar-se de modo inidôneo; fazer declaração falsa ou cometer fraude fiscal ficará impedido de licitar e contratar com a União, e será descredenciado do Sistema de Cadastramento Unificado de Fornecedores – SICAF pelo prazo de até cinco anos, sem prejuízo da multas

previstas em edital e no contrato e das demais cominações legais, conforme disposto no artigo 28 do Decreto nº 5450/2005.

13.3 Das penalidades aplicadas caberá RECURSO, no prazo de 05 (cinco) dias úteis, observados o procedimento estabelecido no artigo 109 da Lei nº 8.666/93, dirigido à autoridade superior por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão.

13.4 Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a CONTRATADA pela sua diferença que será descontada dos pagamentos eventualmente devidos pela VALEC ou cobrada judicialmente;

13.5 As penalidades serão obrigatoriamente registradas no SICAF e, no caso de suspensão de licitar, a CONTRATADA deverá ser descredenciada por igual período, sem prejuízo das multas previstas no Termo de Referência e das demais cominações legais;

13.6 As multas aplicadas deverão ser recolhidas no prazo de 05 (cinco) dias, a contar da data da notificação, podendo a Administração descontar o seu valor da Nota Fiscal ou Documento de Cobrança, independente de notificação, por ocasião de seu pagamento, ou cobrá-las judicialmente, segundo da Lei nº. 6.830/80, com os encargos correspondentes.

14. CRITÉRIOS TÉCNICOS E JULGAMENTO DAS PROPOSTAS

14.1. CRITÉRIOS DE JULGAMENTO

14.1.1. O critério de julgamento será o menor valor por lote.

14.2. CRITÉRIOS TÉCNICOS

14.2.1. Atestado de capacidade técnica, expedido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu bens de natureza similar ao da presente licitação.

14.2.2. Serão considerados compatíveis os atestados que digam respeito a fornecimento de appliances de firewall em qualquer quantidade, acompanhados do respectivo software de gerência

14.2.3. Apresentação, no envio da proposta comercial, comprovante de que a CONTRATADA é fabricante da Solução ou subsidiária brasileira do fabricante ou, ainda, que está credenciada pelo fabricante/subsidiária a comercializar licenças e implantar no Brasil o software/hardware ofertado, bem como autorizada a conceder o direito de utilização do produto contratado.

14.2.4. Apresentar, no envio da proposta comercial, ao menos dois profissionais certificados pelo fabricante da solução, estado esses aptos e autorizados a instalar, configurar e prestar manutenção nos equipamentos e softwares fornecidos.

14.2.5. O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento destes requisitos implicará na desclassificação da proposta.

Item	Link	Documento	Página	Localização

15. CONSÓRCIOS E COOPERATIVAS

15.1. É vedada a participação de consórcios ou cooperativas de empresas, quaisquer que sejam suas formas de constituição, dadas as características específicas da contratação dos produtos e serviços a serem fornecidos, que não pressupõem multiplicidade de atividades empresariais distintas.

16. SUBCONTRATAÇÃO

16.1. Será permitida a subcontratação para a execução dos serviços e fornecimento de bens somente de empresas pertencentes à rede autorizada do fabricante dos sistemas.

16.2. Será observado o limite de subcontratação em 30% do valor do lote.

17. VISTORIA TÉCNICA

17.1. Não será obrigatória, mas será permitida a vistoria técnica, desde que agendada na GEINF/SUPTI/DIPLAN/VALEC, com antecedência de 48h úteis.

18. AMOSTRAS

18.1. Não será obrigatória a entrega de amostras para esse tipo de contratação.

19. ADEQUAÇÃO ORÇAMENTÁRIA

19.1. As despesas decorrentes do fornecimento, objeto deste projeto, correrão à conta do orçamento fiscal e da seguridade social.

20. CRONOGRAMA DE DESEMBOLSO

20.1. O pagamento dos produtos será efetuado a CONTRATADA em parcela única no prazo máximo de até 30 (trinta) dias, contados da data do aceite definitivo da ordem de serviço, de acordo com as exigências administrativas em vigor.

20.2. O pagamento dos serviços, suporte técnico especializado, será efetuado a CONTRATADA, sob demanda, no prazo máximo de até 30 (trinta) dias, contados da data do aceite definitivo da ordem de serviço, de acordo com as exigências administrativas em vigor.

20.3. A Nota Fiscal/Fatura deverá ser acompanhada das seguintes documentações:

20.4. Regularidade junto à Seguridade Social (CND), ao Fundo de Garantia por Tempo de Serviço (CRF) e às Fazendas Federal, Estadual e Municipal de seu domicílio ou sede, por meio de consulta on-line junto ao SICAF.

20.5. Documentos comprobatórios do cumprimento das obrigações decorrentes do contrato.

20.6. O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente na nota fiscal apresentada.

20.7. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

20.8. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

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

20.10. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

20.11. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

20.12. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade da CONTRATANTE, não será rescindido o contrato em execução com a CONTRATADA inadimplente no SICAF.

20.13. Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP, onde:
EM = Encargos moratórios.
N = Número de dias entre a data prevista para pagamento e a do efetivo pagamento.
VP = Valor da parcela a ser paga.
I = Índice de compensação financeira = 0,00016438, sendo assim apurado.
I = (TX).
I = (6/100)/365 , I = 0,00016438.
TX = Percentual de taxa anual = 6%.

20.14. No caso de incorreção nos documentos apresentados, inclusive na NotaFiscal/Fatura, serão os mesmos restituídos à CONTRATADA para as correções necessárias, não respondendo o MMA por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

Integrante Requisitante	Integrante Técnico	Integrante Administrativo
Carlos Soares Sant´Anna Matrícula: 2335960	Rodrigo Gonçalves Pontes Matrícula: 2688179	Anderson Leonir Ahlert Matrícula: 1776055

ANEXO I – ESPECIFICAÇÕES TÉCNICAS

LOTE 1 – SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO FÍSICO

21. REQUISITOS GERAIS

21.1. A solução poderá ser composta de hardware e/ou softwares de diferentes fabricantes, desde que atendidos todos os requisites de integração e performance apresentados.

21.2. Toda solução deverá ser fornecida e instalada e possuir garantia do fabricante pelo período de 48 meses contra falhas em todos os seus componentes

21.3. Deverá ser fornecido transferência de conhecimento de no mínimo 20 horas, para até quatro pessoas, designadas pela Contratante, em até 15 dias após o término da instalação, afim de repassar as informações necessárias dos produtos adquiridos, incluindo detalhamento do produto e seus aspectos gerais de configuração e operação. Esse item será medido conforme avaliação constante no Anexo II.

22. MÓDULO DE CONTROLE DE PERÍMETRO FÍSICO

22.1. O módulo de segurança deve possuir a capacidade e as características abaixo, por equipamento:

22.1.1. Performance mínima de:

22.1.1.1. 16 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

22.1.1.2. 8 Gbps com as seguintes funcionalidade habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

22.1.2. Condições de avaliação de performance:

22.1.2.1. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend/enterprise traffic mix);

22.2. Não será aceito aceleração de pacotes na placa de rede limitando a análise somente até camada 4.

22.3. Suporte a, no mínimo, 3,8 milhões de conexões simultâneas;

22.4. Suporte a, no mínimo, 110 mil novas conexões HTTP por segundo;

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

22.6. Disco Solid State Drive (SSD) redundante de, no mínimo, 220 GB.

22.7. Discos de, no mínimo, 2 TB em RAID 1 para armazenamento de logs interno ou externo a solução de firewall;

22.8. Possuir ao menos 24 interfaces de rede nas seguintes quantidades mínimas:

22.8.1. 04 (quatro) interfaces de rede 1 Gbps em portas cobre;

22.8.2. 08 (oito) interfaces de rede 1 Gbps SFP;

22.8.3. 08 (oito) interfaces de rede 10 Gbps SFP+;

22.8.4. 02 (duas) interfaces dedicadas para alta disponibilidade sendo pelo menos do tipo 10 Gbps;

22.8.5. 01 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

22.8.6. 01 (uma) interface do tipo console ou similar;

22.9. Todas os módulos para as interfaces referentes aos itens 19.8.2 e 19.8.3, deverá ser fornecida aos pares do mesmo modelo e fabricante.

22.10. Suporte a, no mínimo, 15 (quinze) roteadores virtuais;

22.11. Suporte a, no mínimo, 60 (sessenta) zonas de segurança;

22.12. Estar licenciada para ou suportar sem o uso de licença, 10.000 (dez mil) clientes de VPN SSL simultâneos e3.000 (três mil) túneis de VPN IPSEC simultâneos;

22.13. Deve suportar, no mínimo, 10 sistemas virtuais lógicos (Contextos) no firewall Físico;

22.14. Deve permitir expansão futura a até 20 sistemas virtuais lógicos (Contextos) no firewall Físico;

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

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

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

22.18. A console de gerência e monitoração podem residir na mesma solução de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;

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

CARACTERÍSTICAS GERAIS:

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

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

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

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

22.24. O software deverá ser fornecido em sua versão mais atualizada;

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

22.25.1. Suporte a 4094 VLAN Tags 802.1q;

22.25.2. Agregação de links 802.3ad e LACP;

22.25.3. Policy based routing ou policy based forwarding;

22.25.4. Roteamento multicast (PIM-SM);

22.25.5. DHCP Relay e Server;

22.25.6. Jumbo Frames;

22.25.7. Suporte à criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

22.26. Suportar sub-interfaces ethernet logicas;

22.27. O firewall deve ter a capacidade de testar o funcionamento de rotas estáticas e rota default com a definição de um endereço IP de destino que deve estar comunicável através de uma rota. Caso haja falha na comunicação o firewall deve ter a capacidade de usar rota alternativa para estabelecer a comunicação;

22.28. Deve suportar os seguintes tipos de NAT:

22.28.1. Nat dinâmico (Many-to-1) e (Many-to-Many);

22.28.2. Nat estático (1-to-1), (Many-to-Many) e bidirecional 1-to-1;

22.28.3. Tradução de porta (PAT);

22.28.4. Suportar NAT de Origem e Destino de forma independente e/ou simultaneamente;

22.28.5. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

22.29. Deve implementar o protocolo ECMP;

22.29.1. Deve implementar balanceamento de link:

22.29.1.1. Por hash do IP de origem e destino;
22.29.1.2. através do método round-robin;
22.29.1.3. por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quarto links;
22.29.1.4. através de políticas por usuário e grupos de usuários do LDAP/AD;
22.29.1.5. através de políticas por aplicação e porta de destino;

22.30. Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que a plataforma e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pela plataforma devem ser acessíveis via SNMP;

22.31. Enviar log para sistemas de monitoração externos, simultaneamente;

22.32. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

22.33. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

22.34. Proteção contra anti-spoofing;

22.35. Deve permitir bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;

22.36. Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;

22.37. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;

22.38. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

22.39. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

22.40. Suportar a OSPF graceful restart;

22.41. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;

22.42. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra

DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, VPN SSL, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, Neighbor Discovery (ND), Recursive DNS Server (RDNSS), DNS Search List (DNSSL) e controle de aplicação;

22.43. O dispositivos de proteção devem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);

22.43.1. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

22.43.2. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;

22.43.3. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;

22.43.4. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

22.44. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:

22.45. Em modo transparente;

22.46. Em layer 3;

22.47. A configuração em alta disponibilidade deve sincronizar:

22.48. Sessões;

22.49. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;

22.50. Certificados de-criptografados;

22.51. Associações de Segurança das VPNs;

22.52. Tabelas FIB;

22.53. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

22.54. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

CONTROLE POR POLÍTICA DE PROTEÇÃO DE ACESSO

22.55. Deverá suportar controles por zona de segurança.

22.56. Controles de políticas por porta e protocolo.

22.57. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

22.58. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

22.59. Deve suportar a consulta a fontes externas de endereços IP, domínios e URLs podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego;

22.59.1. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

22.59.2. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

22.60. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

22.61. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

22.62. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);

22.63. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

22.64. Deve de-criptografar sites e aplicações que utilizam certificados ECC, incluindo Elliptical Curve Digital Signature Algorithm (ECDSA);

22.65. Controle de inspeção e de-criptografia de SSH por política;

22.66. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;

22.67. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);

22.67.1. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para a plataforma de segurança, quanto para as soluções de análise.

22.68. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg

22.69. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)

22.70. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

22.71. Suporte a objetos e regras IPV6.

22.72. Suporte a objetos e regras multicast.

22.73. Deve suportar no mínino três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;

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

CONTROLE DE APLICAÇÕES

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

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

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

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

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

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

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

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

22.83. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo

também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

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

22.85. Identificar o uso de táticas evasivas via comunicações criptografadas;

22.86. Atualizar a base de assinaturas de aplicações automaticamente;

22.87. Reconhecer aplicações em IPv6;

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

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

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

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

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

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

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

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

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

22.97. Deve alertar o usuário quando uma aplicação for bloqueada;

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

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

22.100. Deve possibilitar a diferenciação:

22.100.1. de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;

22.100.2. de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

22.100.3. de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;

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

22.101.1. Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).

22.101.2. Nível de risco da aplicação.

22.101.3. Categoria e sub-categoria de aplicações.

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

PREVENÇÃO DE AMEAÇAS

22.102. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio plataforma de segurança ou entregue através de composição com outro equipamento ou fabricante.

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

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

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

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

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

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

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

22.110. Deve permitir o bloqueio de vulnerabilidades e exploits conhecidos.

22.111. Deve incluir proteção contra ataques de negação de serviços.

22.112. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelados pelos protocolos GRE e IPSEC não criptografado;

22.113. Deverá possuir os seguintes mecanismos de inspeção de IPS:

22.113.1. Análise de padrões de estado de conexões;

22.113.2. Análise de decodificação de protocolo;

22.113.3. Análise para detecção de anomalias de protocolo;

22.113.4. Análise heurística;

22.113.5. IP Defragmentation;

22.113.6. Remontagem de pacotes de TCP;

22.113.7. Bloqueio de pacotes malformados.

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

22.115. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

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

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

22.118. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

22.119. Possuir assinaturas para bloqueio de ataques de buffer overflow;

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

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

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

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

22.123. Suportar bloqueio de arquivos por tipo;

22.124. Identificar e bloquear comunicação com botnets;

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

22.126. Deve suportar referencia cruzada com CVE;

22.127. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

22.127.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

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

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

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

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

22.132. Os eventos devem identificar o país de onde partiu a ameaça;

22.133. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

22.134. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.

22.135. Rastreamento de vírus em pdf.

22.136. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

22.137. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em politicas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada regra de firewall poderá ter uma configuração diferentes de IPS, sendo essas politicas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

ANÁLISE DE MALWARES MODERNOS

22.138. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

22.139. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

22.140. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;

22.141. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

22.142. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

22.143. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);

22.144. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de mplementação: sniffer, transparente e L3;

22.145. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

22.146. A análise de links em sand-box deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

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

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

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

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

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

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

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

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

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

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

22.157. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class), Android APKs MacOS (mach-O, DMG e PKG) no ambiente de sandbox;

22.158. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos;

22.159. Permitir o envio de arquivos e links para análise no ambiente controlado de forma automática via API.

22.160. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

FILTRO DE URL

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

22.162. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

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

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

22.165. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

22.166. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

22.167. Suportar base ou cache de URLs local na plataforma, evitando delay de comunicação/validação das URLs;

22.168. Possui pelo menos 60 categorias de URLs;

22.169. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

22.170. Suporta a criação categorias de URLs customizadas;

22.171. Suporta a exclusão de URLs do bloqueio, por categoria;

22.172. Permite a customização de página de bloqueio;

22.173. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com Active Directory submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do Active Directory só possam enviar informações de login para sites autorizados na solução;

22.174. Deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas credencias em sites classificados como phishing pelo filtro de URL da solução;

22.175. Permite o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para permitir o usuário continuar acessando o site);

22.176. A funcionalidade de Filtro de URL deve operar em caráter permanente, para base ou cache instalado na solução até a data de vencimento da licença, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

22.177. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

22.178. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

IDENTIFICAÇÃO DE USUÁRIOS

22.179. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com

serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

22.180. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

22.181. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários;

22.182. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

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

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

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

22.185. Suporte a autenticação Kerberos;

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

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

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

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

22.190. O firewall deve operar/suportar Security Assertion Markup Language (SAML) 2.0, com single sign-on e single logout para as funcionalidades de Captive Portal e VPN SSL (client to server), permitindo login único e interativo para fornecer acesso automático a serviços autenticados, internos e externos a organização;

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

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

CONTROLE DE TRÁFEGO E QUALIDADE DE SERVIÇO

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

22.194. Suportar a criação de políticas de QoS por:

22.194.1. Endereço de origem e destino;

22.194.2. Por usuário e grupo do LDAP/AD.

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

22.194.4. Por porta;

22.194.5. O QoS deve possibilitar a definição de classes por Banda Garantida, Banda Máxima e Fila de Prioridade.

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

22.196. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

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

22.198. Disponibilizar estatísticas RealTime para classes de QoS.

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

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

FUNCIONALIDADES DE FILTRO DE DADOS

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

22.202. Os arquivos devem ser identificados por extensão e assinaturas;

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

22.204. Suportar identificação de arquivos compactados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

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

22.206. Permitir listar o número de aplicações suportadas para controle de dados;

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

FUNCIONALIDADES DE GEO-LOCALIZAÇÃO

22.208. Suportar a criação de políticas por Geo Localização, permitindo o tráfego de determinado Pais/Países sejam bloqueados.

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

22.210. Deve permitir visualizar nos logs e criar políticas para liberar e bloquear tráfego de países por: tipo de arquivo, aplicação e categoria de URL;

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

FUNCIONALIDADE DE REDES PRIVADAS VIRTUAIS

22.212. Suportar VPN Site-to-Site e Cliente-To-Site;

22.213. Suportar IPSec VPN;

22.214. Suportar SSL VPN;

22.215. A VPN IPSEc deve suportar:

22.215.1. DES e 3DES;

22.215.2. Autenticação MD5 e SHA-1;

22.215.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;

22.215.4. Algoritmo Internet Key Exchange (IKEv1 e v2);

22.215.5. AES 128, 192 e 256 (Advanced Encryption Standard)

22.215.6. Autenticação via certificado IKE PKI.

22.215.7. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Checkpoint, Juniper, Palo Alto Networks, Fortinet e Sonic Wall;

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

22.217. A VPN SSL deve suportar:

22.217.1. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

22.217.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

22.217.3. Atribuição de endereço IP nos clientes remotos de VPN SSL;

22.217.4. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;

22.217.5. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;

22.217.6. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

22.217.7. Atribuição de DNS nos clientes remotos de VPN;

22.217.8. Deve permitir que seja definido métodos de autenticação distintos por sistema operacional do dispositivo remoto de VPN (Android, IOS, Mac e Windows);

22.217.9. A solução de VPN deve verificar se o client que está conectando é o mesmo para o qual o certificado foi emitido inicialmente. O acesso deve ser bloqueado caso o dispositivo não seja o correto;

22.217.10. Através do agente, deve possibilitar o bloqueio de dispositivos que forem reportados como roubado ou perdido pelo usuário;

22.217.11. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;

22.217.12. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;

22.217.13. Deve avisar ao usuário remoto de VPN quanto a proximidade da expiração de senha LDAP. Deve permitir também a customização da mensagem com informações relevantes para o usuário;

22.217.14. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

22.217.15. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;

22.217.16. Suportar autenticação via AD/LDAP, OTP (One Time Password), certificado e base de usuários local;

22.217.17. Deve permitir a distribuição de certificado para o usuário de remoto através do portal de VPN de forma automatizada;

22.217.18. Deve possuir lista de bloqueio para dispositivos em casos quando, por exemplo, o usuário reportar que o dispositivo foi perdido ou roubado;

22.217.19. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;

22.217.20. Suporta leitura e verificação de CRL (certificate revocation list);

22.217.21. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

22.217.22. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

22.217.23. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário,

22.217.24. Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

22.217.25. Antes do usuário autenticar na estação;

22.217.26. Após autenticação do usuário na estação;

22.217.27. Sob demanda do usuário;

22.217.28. Deverá manter uma conexão segura com o portal durante a sessão.

22.217.29. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8 e Mac OSx;

22.217.30. O cliente de VPN SSL cliente-to-site também deve suportar dispositivos móveis (IOS e ANDROID);

22.217.31. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto;

22.217.32. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e patches instalados, antivírus e versão instalada, firewall no host, criptografia do disco, agente de DLP instalado, backup de disco, chaves de registros e processos ativos;

22.217.33. Deve ser possível a criação de perfis customizados de conformidade com, no mínimo, as seguintes opções: sistema operacional e patches instalados, antivírus e versão instalada,

firewall no host, criptografia do disco, agente de DLP instalado backup de disco, chaves de registros e processos ativos;

22.217.34. O portal de VPN deve enviar ao cliente remoto, a lista de gateways de VPN ativos para estabelecimento da conexão, os quais devem poder ser administrados centralmente;

22.217.35. Deve haver a opção do cliente remoto escolher manualmente o gateway de VPN e de forma automática através da melhor rota entre os gateways disponíveis com base no tempo de resposta mais rápido;

22.217.36. Deve possuir a capacidade de identificar se a origem da conexão de VPN é externa ou interna;

CONSOLE DE GERÊNCIA E MONITORAÇÃO

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

22.219. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

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

22.221. O gerenciamento deve permitir/possuir:

22.221.1. Criação e administração de políticas de firewall e controle de aplicação;

22.221.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

22.221.3. Criação e administração de políticas de Filtro de URL;

22.221.4. Monitoração de logs;

22.221.5. Ferramentas de investigação de logs;

22.221.6. Debugging;

22.221.7. Captura de pacotes.

22.222. Acesso concorrente de administradores;

22.223. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

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

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

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

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

22.228. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas, estatísticas/taxa de logs, uso de disco, período de retenção dos logs e status do envio de logs para soluções externas;

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

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

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

22.232. Autenticação integrada ao Microsoft Active Directory e servidor Radius;

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

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

22.235. Criação de regras que fiquem ativas em horário definido;

22.236. Criação de regras com data de expiração;

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

22.238. Suportar Rollback de Sistema Operacional para a ultima versão local;

22.239. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

22.240. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;

22.241. Validação de regras antes da aplicação;

22.242. Deve implementar mecanismo de validação de configurações antes da aplicação das mesmas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.

22.242.1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

22.242.2. Validação da políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

22.242.3. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

22.243. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

22.244. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

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

22.246. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

22.247. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

22.248. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

22.249. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;

22.250. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;

22.251. Dever permitir a visualização dos logs de malwares modernos, tráfego (IP de origem, destino, usuário e porta), aplicação, IPS, antivírus, anti-spyware, Filtro de URL e filtro de arquivos em uma única tela.

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

22.253. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;

22.254. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

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

22.256. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;

22.257. Os relatórios de visibilidade e uso sobre aplicativos (SaaS) devem poder ser extraídos por grupo de usuários apresentando o uso e consumo de aplicações por grupo de usuário;

22.258. Deve ser possível exportar os logs em CSV;

22.259. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

22.260. Rotação do log;

22.261. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

22.262. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

22.263. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

22.263.1. Situação do dispositivo e do cluster;

22.263.2. Principais aplicações;

22.263.3. Principais aplicações por risco;

22.263.4. Administradores autenticados na gerência da plataforma de segurança;

22.263.5. Número de sessões simultâneas;

22.263.6. Status das interfaces;

22.263.7. Uso de CPU;

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

22.264.1. Resumo gráfico de aplicações utilizadas;

22.264.2. Principais aplicações por utilização de largura de banda de entrada e saída;

22.264.3. Principais aplicações por taxa de transferência de bytes;

22.264.4. Principais hosts por número de ameaças identificadas;

22.264.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

22.264.6. Deve permitir a criação de relatórios personalizados;

22.265. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

22.266. Gerar alertas automáticos via Email, SNMP e Syslog;

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

23. MÓDULO DE PROTEÇÃO À USUÁRIOS E SERVIDORES CRÍTICOS

CARACTERÍSTICAS GERAIS

23.1. Deverá oferecer proteção de estações de trabalho e/ou servidores de rede no combate a vírus, malware, vulnerabilidades conhecidas e desconhecidas;

23.2. A solução deve ser expansível podendo:

23.2.1. Aumentar sua capacidade de tratamento de tráfego com adição de novas de licenças;

23.2.2. A quantidade mínima, para aquisição, deverá ser de 200 (duzentas) licenças para estações de trabalho ou 50 (cinquenta) licenças para servidores.

23.3. As funcionalidades de proteção que compõe a solução de segurança, podem funcionar em múltiplos equipamentos e/ou softwares desde que obedeçam a todos os requisitos desta especificação;

23.4. A solução deverá proporcionar capacidade de gestão centralizada de políticas, logs e relatórios;

FUNCIONALIDADES DE GERENCIAMENTO

23.5. A solução proposta deve ser gerenciada a partir de console única do tipo Interface Gráfica de Usuário (GUI) baseada na Web ou cliente;

23.6. Caso a administração da solução seja via cliente deverá ser compatível com, no mínimo, os sistemas operacionais Windows e Linux;

23.7. Caso a administração da solução seja via browser deverá ser compatível com, no mínimo, Firefox, Chrome e Internet Explorer;

23.8. A solução proposta deverá ter uma arquitetura de gerenciamento multicamadas que consista de Console de Gerenciamento, binários ou serviços e Banco de Dados. A solução deve fornecer opção para instalar os três componentes em um único hardware ou implementações distribuídas de acordo com a necessidade de escalabilidade do parque de máquinas protegidas;

23.9. Caso a solução necessite de Banco de Dados (Ex. SQL Server Enterprise), deverão estar inclusas em sua proposta as licenças necessárias para pleno funcionamento;

23.10. A solução proposta deve ser capaz de instalar vários servidores de gerenciamento para implantações distribuídas e ainda ser gerenciada por uma única console web centralizada;

23.11. A solução proposta deve permitir implementação em ambiente virtual sendo, no mínimo, compatível com VMware;

23.12. O servidor de gerenciamento deverá possuir compatibilidade para instalação nos sistemas operacionais Microsoft Windows Server 2003 R2, SP1 ou superior e Microsoft Windows Server 2008, 2008 R2 ou superior;

23.13. Mecanismo de comunicação randômico (via pull) em tempo determinado pelo administrador entre o cliente e servidor, para consulta de novas configurações e assinaturas evitando sobrecarga de rede e servidor;

23.14. Integração completa ao serviço de diretórios Active Directory (AD), da Microsoft;

23.15. Possibilidade de agrupamento, com base nos objetos do AD, das estações de trabalho e servidores, e definição de políticas por grupos;

23.16. Permitir a divisão lógica dos computadores, dentro da estrutura de gerenciamento, em sites, domínios e grupos, com administração individualizada por domínio;

23.17. O módulo de gestão da solução deve permitir autenticação integrada ao Active Directory;

23.18. Deve permitir a criação de, no mínimo, três perfis de acesso distintos para os usuários administradores da solução;

23.19. Deve registrar nos logs as alterações realizadas pelos administradores na solução;

23.20. A solução proposta deve ser capaz de exportar seus logs no formato syslog para outras soluções de gerenciamento de logs;

23.21. Instalação e atualização do software sem a intervenção do usuário;

23.22. Deve permitir integração com soluções de SIEM enviando logs no formato Syslog ou compatível;

23.23. Deve permitir notificar eventos ao administrador por e-mail;

23.24. Deve permitir a criação de políticas para controle de Vulnerabilidades, Malwares e Restrições de execução por diretório;

23.25. Log centralizado dos eventos de segurança detectados nos endpoints;

23.26. Deve identificar e gerar log de qualquer interferência no serviço de endpoint na máquina afetada, como por exemplo:

23.26.1. Tentativa de shutdown do processo de endpoint;

23.26.2. Tentativa de shutdown do serviço de endpoint;

23.26.3. Logs de sistema relacionados.

23.27. A solução proposta deve permitir o ajuste das políticas forenses dentro do servidor de gerenciamento centralizado com granularidade para definição do tipo de informações forenses a serem coletadas quando ocorrer uma ameaça;

23.28. Deve suportar e possuir agente para pelo menos os seguintes sistemas operacionais:

23.28.1. Windows XP (32-bit e/ou 64-bit, SP3 ou posterior);

23.28.2. Windows 7 (32-bit, 64-bit, RTM e SP1);

23.28.3. Windows 8 (32-bit e 64-bit);

23.28.4. Windows 8.1 (32-bit e 64-bit);

23.28.5. Windows Server 2003 (32-bit e SP2 ou posterior);

23.28.6. Windows Server 2003 R2 (32-bit, SP2 ou posterior);

23.28.7. Windows Server 2008 (32-bit e 64-bit);

23.28.8. Windows Server 2012 (todas as versões);

23.28.9. Windows Server 2012 R2 (todas as versões);

23.28.10. Windows Vista (32-bit, 64-bit e SP2);

23.28.11. Windows 10 RTM (32-bit e 64-bit)

23.29. Deve suportar e possuir agente para maquinas virtuais instaladas em pelo menos:

23.29.1. 1. Citrix Xenserver;

23.29.2. 2. Vmware ESX;

23.30. Proteção contra desinstalação não autorizada dos agentes de endpoint que compõem a solução;

23.31. Proteção contra a desativação não autorizada dos serviços que compõem a solução;

23.32. Ser eficaz na prevenção de Vulnerabilidades e Malwares mesmo quando estiver sem conectividade com servidores de gerenciamento e/ou recursos baseados em nuvem;

23.33. O agente de endpoint deve continuar funcionando a aplicando políticas de controle mesmo se houver interrupção da comunicação com o gerenciamento centralizado;

23.34. Impedir executável malicioso, sem requerer nenhum conhecimento prévio do artefato;

23.35. Possibilidade de colocar arquivos, diretórios e processos em listas de exclusões para não serem verificados pela proteção em tempo real;

23.36. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;

23.37. A solução proposta deve permitir implementação em modo de monitoramento ou aprendizado do ambiente em fase inicial de instalação;

23.38. A solução proposta não deve utilizar intensivamente os recursos de hardware do endpoint, ou seja, não mais que 1% de CPU e não mais que 70 Mega Bytes de memória RAM;

23.39. A solução proposta deve fornecer a capacidade de configurar listas brancas globais para permitir que determinados arquivos executáveis sejam executados dentro de determinadas condições da instituição;

23.40. A solução proposta deve ter a capacidade de criar a partir de incidentes, uma regra de exceção para permitir que um processo seja executado em um determinado endpoint;

CARACTERÍSTICA DE PROTEÇÃO CONTRA VULNERABILIDADES

23.41. A solução proposta deve suportar a proteção de processo e aplicativos em execução no sistema operacional;

23.42. A solução proposta deve suportar a adição de aplicações proprietárias e personalizadas a lista de aplicações protegidas;

23.43. A solução proposta deve ser capaz de fornecer prevenção em tempo real contra exploração de vulnerabilidades de aplicações, bloqueando em tempo real a exploração, não limitadas a falhas de lógica de software, corrupção de memória, sequestro de DLL, etc.;

23.44. A solução proposta deve ser capaz de proteger contra explorações de quaisquer vulnerabilidades não descobertas (desconhecidas) dos aplicativos através do bloqueio de métodos (técnicas e subtécnicas) utilizados para exploração;

23.45. Ao impedir ou bloquear uma técnica de exploração, a solução proposta deve congelar o processo, coletar informações forenses, de no mínimo, nome do processo, origem e caminho do arquivo, data/hora, dump de memória, versão do SO, usuário, versão vulnerável do aplicativo;

23.46. Ao impedir ou bloquear uma técnica de exploração, a solução proposta deve finalizar apenas o processo específico alvo do ataque;

23.47. A solução proposta deve utilizar módulos de métodos de exploração para prevenir ou bloquear tentativas de exploração. Os módulos de métodos de exploração devem proteger aplicações conhecidas, bem como aplicações desconhecidas e desenvolvidas internamente pela instituição;

23.48. A solução proposta deve ser capaz de criar regras de exclusão para excluir endpoints específicos e processos específicos do log de eventos de ameaças de segurança do console de gerenciamento de solução proposta;

23.49. Suportar detecção e bloqueio de, no mínimo, os seguintes métodos:

23.49.1. Deve ser capaz de impedir execução de dados na memória;

23.49.2. Deve ser capaz de impedir acessos não autorizados a DLLs do sistema;

23.49.3. Deve prevenir utilização de DLLs protegidas com fim de ganhar controle de processos e carregar arquivos CPL (painel de controle) maliciosos;

23.49.4. Deve ser capaz de interromper a ocorrência de heap sprays após detecção de exceções suspeitas ou indicativos de tentativas de exploração no host monitorado;

23.49.5. Deve ser capaz de prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração de processadores de texto;

23.49.6. Deve ser capaz de prevenir processamento incorreto de fontes de texto em documentos e arquivos, técnica comum de exploração de processadores de texto;

23.49.7. Deve ser capaz de prevenir o acionamento de vulnerabilidades que resultem na corrupção da área heap na memoria. Exemplo: “free() double”;

23.49.8. Deve prevenir o uso de novas técnicas que possam evadir o DEP (prevenção de execução de dados em memória) e ASLR (randomização do layout de endereçamento em memória);

23.49.9. Deve obrigar a realocação de módulos do sistema operacional, protegendo-os de tentativas de exploração;

23.49.10. Deve ser capaz de detectar e prevenir instâncias de heap spray usando algoritmo de detecção de aumento de consumo de memória, indicando execução de exploração de vulnerabilidade;

23.49.11. Deve ser capaz de prevenir mapeamento de código no endereço zero (início da memória) do espaço de memória do sistema operacional, dessa forma impedindo uso de explorações de referência nula para execução de código arbitrário, exposição de informações de debug, etc;

23.49.12. Deve ser capaz de proteger o acesso a meta dados de bibliotecas críticas do sistema operacional quando estas são descompactadas em memória;

23.49.13. Deve ser capaz de agir preventivamente contra heap spray ao checar periodicamente a zona .heap da memória virtual;

23.49.14. Deve ser capaz de prevenir a exploração de vulnerabilidade bem-sucedida através da pré-alocação aleatória do layout de memória de processos no sistema operacional;

23.49.15. Deve ser capaz de prevenir uso de programação orientada a retorno (return oriented programming) protegendo APIs (interface de programação de aplicação) usadas em cadeias de ROP e técnicas de exploração usando compilações "Just-in-time" (JIT);

23.49.16. Deve ser capaz de mitigar o abuso e captura das estruturas de gerenciamento de exceções (SEH) em memória, e dessa forma impedindo execução de código malicioso arbitrário no sistema operacional;

23.49.17. Deve ser capaz de reservar e proteger determinadas áreas da memória comumente utilizadas para armazenamento de cargas (payload) e instruções maliciosas usando técnicas como heap spray, por exemplo;

23.49.18. Deve ser capaz de prevenir vulnerabilidades lógicas na estrutura de atalhos (links) de sistemas operacionais Windows, onde o carregamento impróprio de atalhos permite execução arbitrária de código em memória (exemplo: CVE-2015-0096);

23.49.19. Deve ser capaz de prevenir contra vulnerabilidades utilizadas em ataques de escalação de privilégios no sistema operacional explorando a instrução sys.exit para retornar ao nível de execução de usuário, após execução de código em nível de sistema (privilege level 0);

23.49.20. Deve ser capaz de aprimorar ou implementar a randomização do layout de endereços em memória (ASLR), garantindo maior aleatoriedade e robustez. Deve também ser capaz de tornar obrigatório o uso da função ASLR;

CARACTERÍSTICA DE PROTEÇÃO CONTRA MALWARE

23.50. A solução proposta deve suportar a proteção contra a execução de arquivos maliciosos;

23.51. A solução proposta deve fornecer a capacidade de fazer controle e restringir os parâmetros sobre como executáveis podem rodar incluindo proteção contra criação de processos filhos;

23.52. A solução proposta deve ser capaz de fornecer prevenção contra malware desconhecido usando análise dinâmica em ambiente de sandbox. Além disso, deve fornecer veredito com relatório de análise completa com o resultado da análise em sandbox;

23.53. A solução proposta deve fornecer a capacidade de criar exceções para hash específicos de arquivos analisados em nuvem na solução de sandbox;

23.54. A solução proposta deve fornecer a capacidade de impedir a execução de um arquivo quando seu valor de hash for desconhecido pela solução de sandbox do fabricante;

23.55. A solução proposta deve fornecer a capacidade de impedir a execução de um arquivo quando o hash do arquivo for desconhecido por cache local e o mesmo não tiver comunicação com o servidor de gerência;

23.56. Caso um malware seja detectado, deve ser possível o envio do mesmo para quarentena automaticamente através de política pré-definida na gerência centralizada;

23.57. Capacidade de procurar códigos maliciosos pelo tipo real de arquivo e não apenas por sua extensão;

23.58. Deve extrair o hash de arquivos executáveis e verificar se o mesmo já foi analisado na solução de sand-box do fabricante de forma automática sem necessidade de scprits externos ou adaptações não nativas da solução. Caso o malware já tenha apresentado comportamento malicioso em sandbox, o mesmo deve ser impedido de ser executado no endpoint;

23.59. Deve permitir o administrador reportar falsos positivos na análise de malwares em sandbox. A solução deve informar o administrador o resultado desta análise e exibir a correção na gerência da solução;

23.60. Deve avisar o usuário quando a execução de um arquivo for bloqueada incluindo casos quando não houver veredito da sandbox sobre o arquivo e o seu status estiver definido como desconhecido;

23.61. Possibilitar o bloqueio automático de malwares já descobertos através da sandbox do fabricante em outros endpoints/localidades do órgão;

23.62. Restringir execução de arquivos específicos somente em diretórios conhecidos e protegidos, tanto na maquina local quanto em drives remotos.

23.62.1. Prevenir execução de arquivos não assinados.

23.62.2. Prevenir execução de arquivos em mídia externa.

23.62.3. Controlar executáveis não assinados por WhiteLists.

23.62.4. Restringir a execução de processos.

23.62.5. Controlar e limitar a criação de processos filhos.

23.62.6. Deve possibilitar o controle de arquivos:

23.62.7. Conhecidos

23.62.8. Desconhecidos

23.63. Suporte a submissão de arquivos executáveis desconhecidos para análise em sandbox do fabricante automaticamente caso o arquivo não seja conhecido.

23.64. Definir e classificar Hash conhecidos.

CARACTERÍSTICA DE COLETA DE INFORMAÇÕES FORENSE

23.65. A solução proposta deve apresentar na gerência centralizada dados forenses capturados pelo agente de endpoint;

23.66. A solução proposta deve coletar, pelo menos, os seguintes dados no endpoint para análise via gerência centralizada;

23.66.1. Dump de memória;

23.66.2. Arquivos Acessados;

23.66.3. Módulos carregados;

23.66.4. URIs acessadas;

23.66.5. Local de execução do arquivo;

23.66.6. Tempo de execução;

23.66.7. Nome do arquivo;

23.66.8. HASH do arquivo;

23.66.9. Nome do usuário relacionado;

23.66.10. Nome do computador;

23.66.11. Endereço IP;

23.66.12. Versão de sistema operacional;

23.66.13. Histórico de arquivo maliciosos;

CARACTERÍSTICA DE RELATÓRIOS:

23.67. A solução proposta deve fornecer uma visualização Web das ameaças;

23.68. A solução proposta deve suportar exportação no formato CSV dos eventos relacionados a ameaças e ao status do agente de endpoints;

23.69. Capacidade de Geração de relatórios, estatísticos e gráficos contendo no mínimo os seguintes tipos pré-definidos:

23.69.1. As 10 máquinas com maior ocorrência de códigos maliciosos;

23.69.2. Os 10 usuários com maior ocorrência de códigos maliciosos;

23.69.3. Localização dos códigos maliciosos;

23.69.4. Sumários das ações realizadas;

23.69.5. Número de infecções detectadas diário, semanal e mensal;

23.70. Códigos maliciosos detectados;

23.71. A solução proposta deverá ter os seguintes dashboards nativos para monitorar a postura de segurança e o status da instituição:

23.71.1. Relatório de restrição de acesso a arquivos e processos;

23.71.2. Técnicas de Malwares utilizadas;

23.71.3. Técnicas de exploração utilizadas;

23.71.4. Informações Forenses coletadas.

23.72. A solução proposta deverá ter os seguintes dashboards de controle para monitorar a situação dos endpoints da intuição:

23.72.1. Detalhes da saúde dos agentes de endpoints;

23.72.2. Dashboard de controle do histórico de regras dos endpoints;

23.72.3. Dashboard de Controle da Política de Segurança instalada nos endpoints;

23.72.4. Dashboard de controle do histórico de status do serviço do endpoints;

24. MÓDULO DE INTELIGENCIA NO COMBATE À AMEAÇAS

24.1. Deverá ser fornecido, no mínimo, 01 (uma) licença de acesso a portal de inteligência no combate a malwares

24.2. Deve permitir o time de resposta a incidentes identificar se um artefato malicioso de dia zero encontrado na rede faz parte de alguma campanha específica de malware, se foi visto até o momento somente na rede da instituição e se já foi encontrado em outras indústrias/países globalmente;

24.3. Deve ser possível pesquisar por informações sobre malwares encontrados na rede da instituição através de:

24.3.1. Hash dos arquivo

24.3.2. Nome do arquivo

24.3.3. Endereço IP de origem

24.3.4. Endereço IP de destino

24.3.5. URL

24.3.6. Dominio

24.3.7. Aplicação por onde o malware passou

24.3.8. Endereço de email remetente ou destinatário do malware

24.3.9. User Agent

24.3.10. Nome da ameaça

24.3.11. Campanhas específicas de malware

24.3.12. O portal de inteligência deve prover as seguintes informações sobre malwares encontrados globalmente:

24.3.13. Tamanho do arquivo

24.3.14. Hash

24.3.15. País de origem

24.3.16. País de destino

24.3.17. Se o malware descoberto faz parte de alguma campanha específica de ataque

24.3.18. Caso o malware faça parte de alguma campanha, deve ser detalhado qual o objetivo da mesma

24.3.19. Tipos de indústria que já foram alvo do malware. Ex: governo, mercado financeiro, tecnologia, etc

24.3.20. Comportamento malicioso conhecido sobre o malware

24.3.21. Acesso/Alterações nos registros do sistema operacional ocasionadas pelo artefato malicioso

24.3.22. Acesso/Alterações nos processo do sistema operacional ocasionadas pelo artefato malicioso

24.3.23. Acesso/Alterações em arquivos binário ocasionadas pelo artefato malicioso

24.3.24. Tentativas de resolução de domínio realizadas pelo artefato malicioso

24.3.25. Tentativas de gets e post realizadas pelo artefato malicioso

24.3.26. Endereço IP de origem

24.3.27. Endereço IP de destino

24.3.28. URL

24.3.29. Domínio

24.3.30. Aplicação por onde o malware passou

24.3.31. Endereço de email remetente ou destinatário do malware

24.3.32. User Agent

24.3.33. Nome da ameaça

24.3.34. Deve ser possível pesquisar malwares encontrados somente na rede da instituição, somente na mesma indústria do órgão (governo), e globalmente em todos os clientes do fabricante

24.3.35. Relatórios e Dashboard:

24.3.36. Deve exibir a de tendência diária de malware com a quantidade encontrada por dia;

24.3.37. Deve exibir as aplicação que mais trazem malwares para dento da rede da instituição. Ex: Flash, FTP, Navegação WEB pelo Browser, SMTP, HTTP-Proxy, Gmail, etc

24.3.38. Principais malwares encontrados por quantidade no período selecionado

24.3.39. Feeds de informações do fabricante sobre ataques e campanhas descobertas

25. SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO DE PERÍMETRO FÍSICO

25.1. A CONTRATADA responderá por todos indícios de inconformidade e defeitos da solução durante um período de 48 (quarenta e oito) meses, contados a partir da data do aceite final da solução;

25.2. Os serviços de suporte técnico deverão prover obrigatoriamente:

25.2.1. Atualizações corretivas de versões de software disponibilizadas pelo fabricante da solução;

25.2.2. Ajustes e configurações de acordo com manuais e normas técnicas especificadas pelo fabricante;

25.2.3. Demais procedimentos destinados a recolocar a solução em perfeito estado de uso.

25.3. A CONTRATADA deverá fornecer informações sobre resolução de problemas, configuração e administração da solução, além de qualquer outro assunto que tenha por objetivo ajudar a CONTRATANTE a realizar uma melhor utilização da solução;

25.4. Os serviços de assistência técnica deverão ser prestados em regime de 24x7, no local onde a solução se encontrar instalada (on-site), por técnicos da CONTRATADA devidamente habilitados e credenciados, e sem qualquer tipo de ônus para a CONTRATANTE;

25.5. A CONTRATADA deverá disponibilizar canais de atendimento, 24 horas por dia, 7 dias por semana, por meio dos quais a CONTRATANTE realizará a abertura de chamados técnicos;

25.6. Para operacionalização do disposto no item anterior, a CONTRATADA deverá disponibilizar, além de número telefônico, no mínimo, mais um canal de atendimento para abertura de chamados técnicos dentre os seguintes: endereços de correio eletrônico ou sítio da web próprio;

25.7. Cabe à CONTRATADA informar a CONTRATANTE sobre mudança dos canais de atendimento;

25.8. Para cada chamado técnico, a CONTRATANTE deverá informar um número de controle (protocolo) para registro;

25.9. Os chamados técnicos serão categorizados nos níveis de severidade descritos abaixo, devendo ser atendidos nos prazos especificados (tabelas I e II):

TABELA I - Níveis de Severidade dos chamados técnicos	
Nível	Descrição
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis, com degradação de desempenho/funcionalidade ou com ocorrência de mau funcionamento.
3	Serviços disponíveis com ocorrência de alarmes. Consultas sobre problemas, dúvidas gerais sobre a execução de configurações, orientações para administração da solução e demais questionamentos sobre a utilização da solução.

TABELA II - Prazos de atendimento a solução			
Prazos	Níveis de severidade		
	1	2	3
Início do atendimento	2 horas	4 horas	8 horas
Término do atendimento	6 horas	8 horas	72 horas

25.10. Serão considerados, para efeito do nível de serviço exigido:

25.10.1. Início do atendimento: Tempo decorrido entre a abertura do chamado técnico pela CONTRATANTE e o primeiro contato do técnico da CONTRATADA;

25.10.2. Término do atendimento: Tempo decorrido entre a abertura do chamado pela CONTRATANTE e a solução da demanda pela CONTRATADA.

25.11. O atendimento da demanda só será considerado concluído após o aceite formal da equipe técnica da CONTRATANTE. Caso a CONTRATANTE não confirme a conclusão do atendimento, este permanecerá aberto. Nesse caso, a CONTRATANTE fornecerá informações sobre as pendências a serem resolvidas;

25.12. O nível de severidade do chamado será informado pela CONTRATANTE no momento da sua abertura;

25.13. O nível de severidade poderá ser reclassificado pela CONTRATANTE. Caso isso ocorra, haverá nova contagem de prazo, conforme o novo nível de severidade, a partir do momento da ciência à CONTRATADA por meio dos canais de atendimento disponibilizados;

25.14. É necessária autorização da CONTRATANTE para qualquer modificação na solução;

25.15. Caso haja necessidade de manutenção externa de equipamento da solução pela CONTRATADA, esta deverá substituir imediatamente tal equipamento por outro de sua propriedade, com características e capacidades iguais ou superiores, em caráter provisório e temporário, pelo prazo máximo de 30 (trinta) dias corridos, contados a partir da data da substituição;

25.16. Para cada atendimento realizado, a CONTRATADA deverá apresentar um relatório contendo data, hora do chamado, início e término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

25.17. A CONTRATADA deverá restabelecer a solução já instalada, por uma nova com características e capacidades iguais ou superiores, no prazo de 10 (dez) dias úteis, nos seguintes casos:

25.17.1. Extrapolação do prazo de 30 (trinta) dias de reposição temporária de equipamentos no caso de necessidade de manutenção externa, conforme definido em item anterior;

25.17.2. Ocorrência de 04 (quatro) ou mais problemas classificados nos níveis de severidade 1 ou 2 dentro de qualquer período de 30 (trinta) dias;

25.17.3. Ocorrência de 12 (doze) ou mais problemas classificados nos níveis de severidade 1 ou 2 dentro de qualquer período de 180 (cento e oitenta) dias;

25.17.4. Soma dos tempos de paralisação da solução, total ou parcial, por problema de hardware ou software, superior a 48 (quarenta e oito) horas, dentro de qualquer período de 180 (cento e oitenta) dias.

LOTE 2 – SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO VIRTUAL

26. REQUISITOS GERAIS

26.1. A solução deverá ser composta por softwares, desde que atendidos todos os requisitos de integração e performance apresentados.

26.2. Toda solução deverá ser fornecida e instalada e possuir garantia do fabricante pelo período de 48 (quarenta e oito) meses contra falhas em todos os seus componentes

26.3. Deverá ser fornecido transferência de conhecimento de no mínimo 20 horas, para até quatro pessoas, designadas pela Contratante, em até 15 dias após o

término da instalação, afim de repassar as informações necessárias dos produtos adquiridos, incluindo detalhamento do produto e seus aspectos gerais de configuração e operação.

27. MÓDULO DE CONTROLE DE PERÍMETRO VIRTUAL

27.1. Cada módulo deve possuir a capacidade e as características abaixo individualmente:

27.1.1. Throughput de 1.3 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

27.1.2. Throughput de 900 Mbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

27.1.3. Os documentos públicos devem comprovar os throughputs aferidos com tráfego HTTP ou blend de protocolos definidos pelo fabricante como tráfego real (real-word traffic blend/Enterprise Mix);

27.1.4. Suporte a, no mínimo, 800.000 conexões simultâneas;

27.1.5. Deve suportar os drivers vmxnet3 e e1000;

27.2. Por cada módulo que compõe o controle de perímetro virtual, entende-se o software e as licenças necessárias para o seu funcionamento;

27.3. Deve ser possível definir interfaces de rede dedicada para gerência do módulo virtual;

27.4. Deve suportar adição de, no mínimo, 4 vCPUs para cada módulo virtual;

27.5. Deve suportar adição de, no mínimo, 9 GB de memória RAM para cada módulo virtual;

CARACTERÍSTICAS GERAIS

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

27.7. O módulo deve ser otimizada para análise de conteúdo de aplicações em camada 7;

27.8. Os módulos virtuais que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, devem ser de um mesmo fabricante;

27.9. O software deverá ser fornecido em sua versão mais atualizada;

27.10. Enviar log para sistemas de monitoração externos, simultaneamente;

27.11. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;

27.12. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;

27.13. Deve possuir proteção anti-spoofing;

27.14. As funcionalidades de controle de aplicações, QOS, SSL e SSH Decryption devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

CARACTERÍSTICAS DE INTEGRAÇÃO COM PLATAFORMA DE VIRTUALIZAÇÃO

27.15. A módulo virtual deve ser do tipo “host-based”, ou seja, módulo virtual virtual compatível com (VMware ESXi) e integrável de forma nativa com o (VMware NSX);

27.16. Deve inspecionar e controlar o tráfego entre máquinas virtuais em uma mesma sub-net através de integração com o VMware NSX sem a necessidade de atribuição de endereços IP nas interfaces do módulo virtual de proteção;

27.17. Deve inspecionar e controlar o tráfego entre máquinas virtuais via software através de integração com o VMware NSX sem a necessidade modificações na topologia de rede do ambiente virtualizado;

27.18. O módulo virtual de proteção deve permitir implementação (multi-tenancy) com criação de pelo menos 30 (trinta) instâncias que separem logicamente tráfegos desejados;

27.19. Deve possuir tabelas de políticas de segurança individualizadas para cada instância criada internamente aos módulos virtuais de proteção;

27.20. O deployment de novos módulos virtuais deve acompanhar o dinamismo do ambiente virtualizado, ou seja, um novo módulo virtual deve ser criado e configurado automaticamente em novos servidores físicos adicionados ao pool automaticamente;

27.21. O módulo virtual de proteção deve estabelecer comunicação com a gerência centralizada da solução para obtenção de licenças e políticas de controle de tráfego de forma automatizada sem a necessidade de intervenção humana no processo;

27.22. Deve suportar implementação com (distributed switch);

27.23. Deve permitir a criação de objetos dinâmicos para servidores virtuais do pool, ou seja, quando uma máquina virtual hospedada em um servidor físico (A) e protegida por um modulo virtual de firewall (A), movimentar-se para um servidor físico (B) o objeto dinâmico deverá ser movido automaticamente para o módulo virtual (B), sem a necessidade de intervenção humana no processo;

27.24. Deve permitir a criação de regras de segurança de firewall camada 7, IPS, antivírus e anti-spyware usando objetos dinâmicos baseados em agrupamento de máquinas por "tag" existentes no Vmware NSX;

27.25. Deve permitir a criação de regras de redirect de tráfego no NSX usando security groups a partir da gerência centralizada da solução de firewall camada 7;

27.26. Deve controlar o tráfego leste/oeste entre máquinas virtuais pertencentes ao pool de servidores estando ou não hospedados no mesmo servido físico;

27.27. Deve possuir API aberta que permita integração com tecnologias de orquestração;

CONTROLE POR POLÍTICA DE FIREWALL

27.28. Deverá suportar controles por zona de segurança.

27.29. Controles de políticas por porta e protocolo.

27.30. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.

27.31. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.

27.32. Deve permitir autenticação segura através de certificado nas fontes externas de endereços IP, domínios e URLs;

27.33. Deve permitir consultar e criar exceção para objetos das listas externas a partir da interface de gerência do próprio firewall;

27.34. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

27.35. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).

27.36. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;

27.37. Controle de inspeção e de-criptografia de SSH por política;

27.38. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg

27.39. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)

27.40. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.

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

CONTROLE DE APLICAÇÕES

27.42. Os módulos virtuais de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

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

27.42.2. Reconhecer pelo menos 1500 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

27.42.3. Deve permitir criação de políticas por aplicação aderentes ao negócio da instituição, incluindo, mas não limitado a:

27.42.3.1. Permitir que somente a aplicação SSH seja utilizada pela equipe de suporte baseado em um grupo de usuários do LDAP/AD;

27.42.3.2. Permitir comunicação entre uma máquina virtual (A) e (B) para apenas uma sub-aplicação do Oracle;

27.42.3.3. Permitir que um determinado grupo de usuários do LDAP/AD tenha acesso restrito a uma sub-aplicação customizada do cliente incluída na base de aplicações da solução

27.42.3.4. Permitir que um determinado grupo de usuários do LDAP/AD acesso total a aplicação;

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

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

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

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

27.43. Para tráfego criptografado (SSL e SSH), deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

27.44. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

27.45. Identificar o uso de táticas evasivas via comunicações criptografadas;

27.46. Atualizar a base de assinaturas de aplicações automaticamente;

27.47. Reconhecer aplicações em IPv6;

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

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

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

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

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

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

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

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

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

27.56. Deve alertar o usuário quando uma aplicação for bloqueada;

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

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

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

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

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

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

27.63. Tecnologia utilizada na aplicações (Client-Server, Browse Based, Network Protocol, etc).

27.64. Nível de risco da aplicação.

27.65. Categoria e sub-categoria de aplicações.

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

PREVENÇÃO DE AMEAÇAS

27.67. Para proteção do ambiente contra ataques, os módulos virtuais devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados ou entregue através de composição com outro fabricante.

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

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

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

27.71. Quando utilizada as funções de IPS, Antivírus e Anti-spyware, o módulo virtual deve entregar a mesma performance (não degradar) entre ter 1 única assinatura de IPS habilitada ou ter todas as assinaturas de IPS, Anti-Vírus e Antispyware habilitadas simultaneamente.

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

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

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

27.75. Deve permitir o bloqueio de vulnerabilidades.

27.76. Deve permitir o bloqueio de exploits conhecidos.

27.77. Deve incluir proteção contra ataques de negação de serviços.

27.78. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelados pelos protocolos GRE e IPSEC não criptografado;

27.79. Deverá possuir os seguintes mecanismos de inspeção de IPS:

27.79.1. Análise de padrões de estado de conexões;

27.79.2. Análise de decodificação de protocolo;

27.79.3. Análise para detecção de anomalias de protocolo;

27.79.4. Análise heurística;

27.79.5. IP Defragmentation;

27.79.6. Remontagem de pacotes de TCP;

27.79.7. Bloqueio de pacotes malformados.

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

27.81. Detectar e bloquear a origem de portscans;

27.82. Detectar e bloquear a origem de portscans com possibilidade de criar exceções para endereços IPs de ferramentas de monitoramento da organização;

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

27.84. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de

protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

27.85. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

27.86. Possuir assinaturas para bloqueio de ataques de buffer overflow;

27.87. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto.

27.88. Permitir o bloqueio de malwares e spywares, pelo menos nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

27.89. Suportar bloqueio de arquivos por tipo;

27.90. Identificar e bloquear comunicação com botnets;

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

27.92. Deve suportar referencia cruzada com CVE;

27.93. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

27.93.1. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo módulo virtual;

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

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

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

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

27.98. Os eventos devem identificar o país de onde partiu a ameaça;

27.99. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.

27.100. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.

27.101. Rastreamento de vírus em pdf.

27.102. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)

27.103. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em politicas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada politica de firewall poderá ter uma configuração diferentes de IPS, sendo essas politicas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

ANÁLISE DE MALWARES MODERNOS

27.104. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;

27.105. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;

27.106. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, tipo de arquivo e todas estas opções simultaneamente;

27.107. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;

27.108. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;

27.109. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);

27.110. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB;

27.111. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;

27.112. A análise de links em sand-box deve deve ser capaz de classificar sites falsos na categoria de phishing e atualizar a base de filtro de URL da solução;

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

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

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

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

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

27.118. Deve permitir visualizar o resultados das análises de malwares de dia zero nos diferentes sistemas operacionais suportados;

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

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

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

27.122. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos java (.jar e class) e Android APKs no ambiente controlado;

27.123. Deve atualizar a base com assinaturas para bloqueio dos malwares identificados em sand-box com frequência de, pelo menos, 5 minutos

27.124. Permitir o envio de arquivos e links para análise no ambiente controlado via de forma automática via API.

27.125. Deve permitir o envio para análise em sand-box de malwares bloqueados pelo antivírus da solução;

IDENTIFICAÇÃO DE USUÁRIOS

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

27.127. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

27.128. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/politicas baseadas em usuários e grupos de usuários.

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

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

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

27.132. Suporte a autenticação Kerberos.

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

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

CONTROLE DE TRÁFEGO E QUALIDADE DE SERVIÇO

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

27.136. Suportar a criação de políticas de QoS por:

27.136.1. Endereço de origem

27.136.2. Endereço de destino

27.136.3. Por usuário e grupo do LDAP/AD.

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

27.136.5. Por porta;

27.137. O QoS deve possibilitar a definição de classes por:

27.137.1. Banda Garantida

27.137.2. Banda Máxima

27.137.3. Fila de Prioridade.

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

27.139. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

27.140. Disponibilizar estatísticas RealTime para classes de QoS.

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

FUNCIONALIDADES DE FILTRO DE DADOS

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

27.143. Os arquivos devem ser identificados por extensão e assinaturas;

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

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

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

27.147. Permitir listar o número de aplicações suportadas para controle de dados;

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

FUNCIONALIDADES DE GEO-LOCALIZAÇÃO

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

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

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

28. MÓDULO DE GERÊNCIA CENTRALIZADO

28.1. Deve permitir o gerenciamento centralizado de diversos módulos virtuais;

28.2. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o trafego que passar pelos módulos virtuais;

28.3. Controle sobre todos os módulos virtuais da plataforma de segurança em uma única console, com administração de privilégios e funções;

28.4. O gerenciamento centralizado poderá ser entregue como appliance físico ou virtual. Caso seja entregue em appliance fisíco deve ser compatível com rack 19 polegadas e possuir todos acessórios necessários para sua instalação. Caso seja entregue em appliance virtual dever ser compatível com VMware ESXi, nesse caso a estrutura de virtualização será fornecida pelo contratante.

28.5. Deve permitir controle global de políticas para todos os módulos virtuais que compõe a plataforma de segurança;

28.6. Deve suportar organizar os módulos virtuais administrados em grupos;

28.7. Deve permitir a criação de objetos e políticas compartilhadas;

28.8. Deve consolidar logs e relatórios de todos os módulos virtuais administrados;

28.9. Deve permitir que exportar backup de configuração automaticamente via agendamento;

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

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

28.12. Deve permitir substituir o certificado de fábrica no acesso HTTPS a gerência do firewall como possibilidade de uso de certificado criado localmente na própria solução ou importado de fonte externa;

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

28.14. O gerenciamento deve permitir/possuir:

28.14.1. Criação e administração de políticas de firewall e controle de aplicação;

28.14.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;

28.14.3. Monitoração de logs;

28.14.4. Ferramentas de investigação de logs;

28.14.5. Debugging;

28.14.6. Captura de pacotes.

28.15. Deve permitir que administradores concorrentes façam modificações, valide configurações e reverta configurações do firewall simultaneamente e que cada administrador consiga aplicar apenas as suas alterações de forma independente das realizadas por outro administrador;

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

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

28.18. Deve permitir monitorar via SNMP uso de recursos por número elevado de sessões, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;

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

28.20. Permitir definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

28.21. Possuir Autenticação integrada ao Microsoft Active Directory e servidor Radius;

28.22. identificar por pesquisa de endereço IP, IP Range, subnet ou objetos, quais as regras que o estão sendo utilizados;

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

28.24. Permitir a criação de regras que fiquem ativas em horário definido;

28.25. Permitir a criação de regras com data de expiração;

28.26. Suportar backup das configurações e rollback de configuração para a última configuração salva;

28.27. Suportar Rollback de Sistema Operacional para a ultima versão local;

28.28. Possuir habilidade de upgrade via SCP, TFTP e interface de gerenciamento;

28.29. Executar a validação de regras antes da sua aplicação;

28.29.1. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.

28.30. Efetuar a validação da políticas, avisando quando houver regras que ofusquem ou conflitem com outras (shadowing);

28.30.1. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

28.31. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.

28.32. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)

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

28.34. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;

28.35. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;

28.36. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware) e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;

28.37. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos módulos virtuais de segurança;

28.38. Deve possuir relatórios de utilização dos recursos por aplicações, ameaças (IPS, Antivírus e Anti-Spware), etc;

28.39. Prover uma visualização sumarizada de todas as aplicações e ameaças (IPS, Antivírus e Anti-Spware), que passaram pela solução;

28.40. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

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

28.42. Deve ser possível exportar os logs em CSV;

28.43. Deverá ser possível acessar o módulo virtual a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do estiver totalmente utilizada.

28.44. Possuir rotação do log;

28.45. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;

28.46. Deve permitir fazer o envio de logs para soluções externas de forma granular podendo selecionar quais campos dos logs serão enviados incluindo, mas não limitado a: tipo de ameaça, usuário, aplicação, etc;

28.47. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):

28.47.1. Situação do módulo virtual e do cluster;

28.47.2. Principais aplicações;

28.47.3. Principais aplicações por risco;

28.47.4. Administradores autenticados na gerência da plataforma de segurança;

28.47.5. Número de sessões simultâneas;

28.47.6. Status das interfaces;

28.47.7. Uso de CPU;

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

28.48.1. Resumo gráfico de aplicações utilizadas;

28.48.2. Principais aplicações por utilização de largura de banda de entrada e saída;

28.48.3. Principais aplicações por taxa de transferência de bytes;

28.48.4. Principais hosts por número de ameaças identificadas;

28.48.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;

28.48.6. Deve permitir a criação de relatórios personalizados;

28.49. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

28.50. Gerar alertas automáticos via:

28.50.1. Email;

28.50.2. SNMP;

28.50.3. Syslog;

29. SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO E GERENCIA CENTRALIZADA DO PERIMETRO VIRTUAL

29.1. A CONTRATADA responderá por todos indícios de inconformidade e defeitos da solução durante um período de 48 (quarenta e oito) meses, contados a partir da data do aceite final da solução;

29.2. Os serviços de suporte técnico deverão prover obrigatoriamente:

29.2.1. Atualizações corretivas de versões de software disponibilizadas pelo fabricante da solução;

29.2.2. Ajustes e configurações de acordo com manuais e normas técnicas especificadas pelo fabricante;

29.2.3. Demais procedimentos destinados a recolocar a solução em perfeito estado de uso.

29.3. A CONTRATADA deverá fornecer informações sobre resolução de problemas, configuração e administração da solução, além de qualquer outro assunto que tenha por objetivo ajudar a CONTRATANTE a realizar uma melhor utilização da solução;

29.4. Os serviços de assistência técnica deverão ser prestados em regime de 24x7, no local onde a solução se encontrar instalada (on-site), por técnicos da

CONTRATADA devidamente habilitados e credenciados, e sem qualquer tipo de ônus para a CONTRATANTE;

29.5. A CONTRATADA deverá disponibilizar canais de atendimento, 24 horas por dia, 7 dias por semana, por meio dos quais a CONTRATANTE realizará a abertura de chamados técnicos;

29.6. Para operacionalização do disposto no item anterior, a CONTRATADA deverá disponibilizar, além de número telefônico, no mínimo, mais um canal de atendimento para abertura de chamados técnicos dentre os seguintes: endereços de correio eletrônico ou sítio da web próprio;

29.7. Cabe à CONTRATADA informar a CONTRATANTE sobre mudança dos canais de atendimento;

29.8. Para cada chamado técnico, a CONTRATANTE deverá informar um número de controle (protocolo) para registro;

29.9. Os chamados técnicos serão categorizados nos níveis de severidade descritos abaixo, devendo ser atendidos nos prazos especificados (tabelas I e II):

TABELA I - Níveis de Severidade dos chamados técnicos	
Nível	**Descrição**
1	Serviços totalmente indisponíveis.
2	Serviços parcialmente indisponíveis, com degradação de desempenho/funcionalidade ou com ocorrência de mau funcionamento.
3	Serviços disponíveis com ocorrência de alarmes. Consultas sobre problemas, dúvidas gerais sobre a execução de configurações, orientações para administração da solução e demais questionamentos sobre a utilização da solução.

TABELA II - Prazos de atendimento a solução			
Prazos	**Níveis de severidade**		
	1	**2**	**3**
Início do atendimento	2 horas	4 horas	8 horas
Término do atendimento	6 horas	8 horas	72 horas

29.10. ***Serão considerados,*** para efeito do nível de serviço exigido:

29.10.1. Início do atendimento: Tempo decorrido entre a abertura do chamado técnico pela CONTRATANTE e o primeiro contato do técnico da CONTRATADA;

29.10.2. Término do atendimento: Tempo decorrido entre a abertura do chamado pela CONTRATANTE e a solução da demanda pela CONTRATADA.

29.11. O atendimento da demanda só será considerado concluído após o aceite formal da equipe técnica da CONTRATANTE. Caso a CONTRATANTE não confirme a conclusão do atendimento, este permanecerá aberto. Nesse caso, a CONTRATANTE fornecerá informações sobre as pendências a serem resolvidas;

29.12. O nível de severidade do chamado será informado pela CONTRATANTE no momento da sua abertura;

29.13. O nível de severidade poderá ser reclassificado pela CONTRATANTE. Caso isso ocorra, haverá nova contagem de prazo, conforme o novo nível de severidade, a partir do momento da ciência à CONTRATADA por meio dos canais de atendimento disponibilizados;

29.14. É necessária autorização da CONTRATANTE para qualquer modificação na solução;

29.15. Caso haja necessidade de manutenção externa de equipamento da solução pela CONTRATADA, esta deverá substituir imediatamente tal equipamento por outro de sua propriedade, com características e capacidades iguais ou superiores, em caráter provisório e temporário, pelo prazo máximo de 30 (trinta) dias corridos, contados a partir da data da substituição;

29.16. Para cada atendimento realizado, a CONTRATADA deverá apresentar um relatório contendo data, hora do chamado, início e término do atendimento, identificação do problema, providências adotadas e demais informações pertinentes;

29.17. A CONTRATADA deverá restabelecer a solução já instalada, por uma nova com características e capacidades iguais ou superiores, no prazo de 10 (dez) dias úteis, nos seguintes casos:

29.17.1. Extrapolação do prazo de 30 (trinta) dias de reposição temporária de equipamentos no caso de necessidade de manutenção externa, conforme definido em item anterior;

29.17.2. Ocorrência de 04 (quatro) ou mais problemas classificados nos níveis de severidade 1 ou 2 dentro de qualquer período de 30 (trinta) dias;

29.17.3. Ocorrência de 12 (doze) ou mais problemas classificados nos níveis de severidade 1 ou 2 dentro de qualquer período de 180 (cento e oitenta) dias;

29.17.4. Soma dos tempos de paralisação da solução, total ou parcial, por problema de hardware ou software, superior a 48 (quarenta e oito) horas, dentro de qualquer período de 180 (cento e oitenta) dias.

30. DOCUMENTOS

30.1. A Licitante deverá apresentar em sua Proposta:

30.1.1. Documento contendo a especificação técnica detalhada do(s) produto(s) cotado(s);

30.1.2. Apresentar, no envio da proposta comercial, ao menos dois profissionais certificados pelo fabricante da solução, estado esses aptos e autorizados a instalar, configurar e prestar manutenção nos equipamentos e softwares fornecidos;

30.1.3. Declaração do fabricante, com referência ao número do Edital, de que a LICITANTE é revenda autorizada de seus produtos, e que está apta a executar os serviços de instalação e suporte técnico;

30.1.4. Todas as características técnicas obrigatórias deverão ser do fabricante e comprovadas por meio de folders, ou catálogos, ou manuais, ou impressão de páginas do fabricante na Internet, os quais deverão ser entregues juntamente com a proposta;

30.1.5. Documento denominado "Atendimento às Especificações" (modelo constante do Anexo III deste Termo de Referência) para demonstrar o atendimento aos subitens constantes no item 3 "Especificação Técnica";

30.1.6. Toda a Proposta Técnica deverá ter uma única numeração sequencial, desde a página inicial até a página final. A numeração deverá estar de forma visível;

31. Propostas

As propostas devem ser enviadas seguindo a tabela abaixo para os lotes distintamente:

LOTE 1 - SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO FÍSICO

ITEM	DESCRIÇÃO DOS ITENS	QTD	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	MÓDULO DE CONTROLE DE PERÍMETRO FÍSICO	2	HARDWARE	R$	R$
2	MÓDULO DE PROTEÇÃO À USUÁRIOS E SERVIDORES CRÍTICOS	1.200	LICENÇA	R$	R$
3	MÓDULO DE INTELIGÊNCIA NO COMBATE À AMEAÇAS	1	LICENÇA	R$	R$
4	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO DE PERÍMETRO FÍSICO	1	SERVIÇO	R$	R$

LOTE 2 - SOLUÇÃO DE PROTEÇÃO DE PERÍMETRO VIRTUAL

ITEM	DESCRIÇÃO DOS ITENS	QTD	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
5	MÓDULO DE CONTROLE DE PERÍMETRO VIRTUAL	4	SOFTWARE	R$	R$
6	MÓDULO DE GERÊNCIA CENTRALIZADO	1	SOFWARE	R$	R$
7	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO E GERÊNCIA CENTRALIZADA DO PERIMETRO VIRTUAL	1	SERVIÇO	R$	R$

ANEXO II
Modelo de questionário de satisfação da Transferência de Conhecimento

FORMULÁRIO DE AVALIAÇÃO

Caro participante,

Este instrumento de avaliação objetiva conhecer o seu grau de satisfação em relação ao curso de que acaba de participar. A sua opinião é fundamental para que possamos melhorar cada vez mais a qualidade dos eventos oferecidos.

Solicitamos que responda às questões a seguir, utilizando a escala abaixo. Não é necessário se identificar.

Discordo totalmente — Concordo totalmente

1 2 3 4 5

I - Quanto ao INSTRUTOR:

1. Domínio do assunto	1	2	3	4	5
2. Clareza e objetividade na exposição do assunto	1	2	3	4	5
3. Utilização de exemplos práticos aplicáveis a VALEC	1	2	3	4	5
4. Administração do tempo previsto	1	2	3	4	5
5. Estímulo à participação do grupo	1	2	3	4	5
6. Flexibilidade nas discussões	1	2	3	4	5
7. Presteza e clareza no atendimento às dúvidas	1	2	3	4	5
8. Organização e didática utilizada	1	2	3	4	5
9. Capacidade de administrar situações imprevistas	1	2	3	4	5
10. Cumprimento do conteúdo proposto	1	2	3	4	5

II- Quanto ao DESEMPENHO PESSOAL:

1. Motivação	1	2	3	4	5
2. Nível de comprometimento	1	2	3	4	5
3. Pontualidade	1	2	3	4	5

III- Quanto ao CONTEÚDO DO EVENTO:

1. Aquisição de novos conhecimentos	1	2	3	4	5
2. Aplicabilidade às atividades desenvolvidas na VALEC	1	2	3	4	5
3. Desenvolvimento do conteúdo	1	2	3	4	5

IV- Quanto à ORGANIZAÇÃO DO EVENTO:

1. Divulgação do curso	1	2	3	4	5
2. Horário de realização	1	2	3	4	5
3. Local de realização	1	2	3	4	5
4. Material didático (apostila, textos, etc.)	1	2	3	4	5
5. Recursos audiovisuais	1	2	3	4	5
6. Equipe de apoio	1	2	3	4	5

V- Quanto à AVALIAÇÃO GERAL:

1. Aproveitamento do curso	1	2	3	4	5
2. Atendimento às expectativas	1	2	3	4	5
3. Coerência entre o proposto e o realizado	1	2	3	4	5
4. Adequação do curso em relação às demandas do trabalho	1	2	3	4	5

Comente sobre o curso:

_____
_____
_____

Apresente suas sugestões, elogios e/ou críticas:

_____
_____
_____

ANEXO III
ATENDIMENTO ÀS ESPECIFICAÇÕES

Demonstramos, em atendimento ao previsto no item..... do edital **VALEC n.º** ....., o atendimento aos itens e subitens obrigatórios especificando a localização exata das informações comprobatórias inseridas em nossa Proposta.

Equipamento (especificar)

Item ou Subitem	Atendimento (Sim ou Não)	Documento	Página

Local e data

Assinatura e carimbo

(Representante Legal)

Observação: Emitir em papel que identifique o **Licitante.**

ANEXO IV – PENALIDADES E MULTAS

DESCRIÇÃO	FAIXA	PENALIDADE
Finalização do Atendimento Remoto	6h < PFA ≤ 12h	Glosa de 1% sobre o valor do equipamento
	12h < PFA ≤ 18h	Glosa de 2%, por hora, sobre o valor do equipamento
	18h < PFA ≤ 24h	Glosa de 1% sobre o valor do contrato + 2%, por hora, sobre o valor do equipamento
	24h < PFA ≤ 30h	Glosa de 2%, por hora, sobre o valor do contrato
	PFA > 30h	**Inexecução Contratual**
Inicialização do atendimento *in loco*	4h < PIA ≤ 8h	Glosa de 1% sobre o valor do equipamento
	8h < PIA ≤ 12h	Glosa de 3%, por hora, sobre o valor do equipamento
	12h < PIA ≤ 16h	Glosa de 1% sobre o valor do contrato + 3%, por hora, sobre o valor do equipamento
	16h < PIA ≤ 20h	Glosa de 3%, por hora, sobre o valor do contrato
	PIA > 20h	**Inexecução Contratual**
Finalização do Atendimento *in loco*/ Rede Autorizada	12h < PFA ≤ 24h	Glosa de 1% sobre o valor do equipamento
	24h < PFA ≤ 36h	Glosa de 1%, por hora, sobre o valor do equipamento
	36h < PFA ≤ 48h	Glosa de 1% sobre o valor do contrato + 1%, por hora, sobre o valor do equipamento
	48h < PFA ≤ 60h	Glosa de 1%, por hora, sobre o valor do contrato
	PFA > 60h	**Inexecução Contratual**

ANEXO V - TERMO DE ACEITE PROVISÓRIO.

IDENTIFICAÇÃO			
CONTRATO:		**N° DA OS / OFB:**	
OBJETO:			
CONTRATANTE:			
CONTRATADA:			

Por este instrumento, atestamos para fins de cumprimento do disposto no artigo 25, inciso III, alínea "a" da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 12/11/2010, que os serviços (ou bens), relacionados na O.S. acima identificada, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo CONTRATANTE. Ressaltamos que o recebimento definitivo destes serviços (ou bens) ocorrerá em até xx dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do Planejamento da Contratação correspondente ao Contrato supracitado.

DE ACORDO	
CONTRATANTE	**CONTRATADA**
_____ ***<Nome>*** **Mat.:**	_____ ***<Nome>*** **Mat.:**

ANEXO VI - TERMO DE ACEITE DEFINITIVO.

IDENTIFICAÇÃO					
CONTRATO:		**N° DA OS / OFB:**		**ITEM:**	
OBJETO:					
GESTOR DO CONTRATO:					
ÁREA REQUISITANTE DA SOLUÇÃO:					

Por este instrumento, as partes acima identificadas atestam para fins de cumprimento do disposto no artigo 25, inciso III, alínea "h" da Instrução Normativa nº 4 do Ministério do Planejamento, Orçamento e Gestão – MPOG, de 12/11/20010, que os serviços (ou bens) identificados acima possuem a qualidade compatível com a especificada no Planejamento da Contratação / Projeto Básico do Contrato supracitado.

DE ACORDO	
CONTRATANTE	**CONTRATADA**
_____ ***<Nome>*** **Mat.:**	_____ ***<Nome>*** **Mat.:**

_____, _____ de _____ de 20_____

ANEXO VII - ORDEM DE FORNECIMENTO DE BENS

Identificação

OFB:		**Requisitante:**		**Data de Emissão:**	
Nome do Projeto:		**Sigla:**		**Emer-gencial:**	**Sim( ) Não ( )**
Contratada:		**Contrato:**			

1 – Especificação dos Produtos e Volumes

Id	PRODUTO	MÉTRICA	QUANT.	PREÇO R$
1				**R$**
2				**R$**
3				**R$**
...				**R$**
TOTAL =				**R$**

2 – Instruções Complementares

Ciência

CONTRATANTE

Gestor do Contrato

_____

<Nome>

Matrícula: *<Matr.>*

CONTRATADA

Preposto

_____

<Nome>

<Qualificação>

_____, _____ de _____ de 20_____

ANEXO VIII – MODELO DE ATESTADO

Atestado para não utilização de produtos perigosos e aderência aos requisitos de sustentabilidade ambiental.

Atestamos, para fins de comprovação junto à VALEC relativamente ao Edital _____ que o Sr. (a) _____ representante da empresa _____ CNPJ _____, atesta para todos os fins que a empresa não emprega substâncias perigosas em seu processo de produção de acordo com as exigências do Edital.

Brasília, _____ de _____ de _____

Representante do Fabricante:

Nome (*): _____

Assinatura: _____

(*) apresentar ato constitutivo que subscreva a pessoa a representar o fabricante

ANEXO IX – TERMO DE CIENCIA

IDENTIFICAÇÃO DO CONTRATO			
Contrato Nº			
Objeto:			
Gestor do Contrato:		Mat.:	
Contratante (Órgão):			
Contratada:		CNPJ	
Preposto da Contratada:		CPF	

Por este instrumento, os funcionários abaixo assinados declaram ter ciência e conhecer a declaração de manutenção de sigilo e das normas de segurança vigentes na Contratante.

Brasília, _____ de_____ _____ de 20_____.

CIÊNCIA	
CONTRATADA	
_____ Mat.: <Nome>	_____ <Nome> Mat.:

_____ <Nome> Mat.:	_____ <Nome> Mat.:

ANEXO X – TERMO DE COMPROMISSO

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

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

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

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

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

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 4.553 de 27/12/2002 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

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

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na

execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

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

I – Sejam comprovadamente de domínio público no momento da revelação;

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

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

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

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

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do

CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

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

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

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

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

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

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

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

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

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

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

Cláusula Quinta – DA VIGÊNCIA

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

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS

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

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

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

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

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

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

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

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

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

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

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

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

Cláusula Oitava – DO FORO

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

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

_____, _____ de _____ de 20____

De Acordo

CONTRATANTE	**CONTRATADA**
_____	_____
<Nome>	***<Nome>***
Matrícula: *<Matr.>*	***<Qualificação>***

Testemunhas

Testemunha 1	**Testemunha 2**
_____	_____
<Nome>	***<Nome>***
<Qualificação>	***<Qualificação>***

ANEXO II

MINUTA DE CONTRATO

CONTRATO nº. ___/2018
PROCESSO nº 51402.180668/2017-96

CONTRATO PARA AQUISIÇÃO DE PLATAFORMA DE SEGURANÇA, QUE ENTRE SI FAZEM A VALEC – ENGENHARIA, CONSTRUÇÕES E FERROVIAS S. A. E _____.

A **VALEC – ENGENHARIA, CONSTRUÇÕES E FERROVIAS S. A.**, empresa pública federal, concessionária de serviço público, vinculada ao Ministério dos Transportes, com sede no Setor de Autarquias Sul (SAUS), Quadra 1, Bloco "G", Lotes 3 e 5, Asa Sul, cidade de Brasília (DF), CEP 70.070-010, inscrita no CNPJ/MF sob o nº. 42.150.664/0001-87, doravante denominada **CONTRATANTE**, neste ato representada por seu Diretor-Presidente, **MÁRIO MONDOLFO**, brasileiro, casado, engenheiro civil, portador da carteira de identidade nº. 6.578.384-0 SSP/SP, inscrito no CPF sob o nº. 913.529.248-20, residente e domiciliado na cidade de São Paulo (SP), e por seu Diretor de Planejamento, **MÁRCIO GUIMARÃES DE AQUINO**, brasileiro, casado, administrador, portador da carteira de identidade nº. 1.561.673-SSP/DF, inscrito no CPF sob o n°. 631.403.497-34, residente e domiciliado na cidade de Brasília (DF), e a **_____**, com sede no endereço **_____**, inscrita no CNPJ/MF sob o nº. **_____**, doravante denominada **CONTRATADA**, neste ato representada por seu representante **_____**, portador da carteira de identidade nº. **_____**, inscrito no CPF sob o nº. **_____**, resolvem celebrar o presente Contrato, mediante as Cláusulas e condições seguintes:

CLÁUSULA PRIMEIRA – OBJETO

1.1 O presente Contrato tem por objeto a aquisição de plataforma de segurança com funcionalidade de proteção à rede, usuários/servidores críticos e inteligência no combate a ameaças, incluindo o fornecimento de equipamentos e *softwares* integrados em forma de *appliance* e/ou *software appliance* (módulo virtual) quando especificado,

serviços de instalação e configuração, suporte técnico e garantia e transferência de conhecimento, conforme especificações constantes no Termo de Referência, anexo do Edital do Pregão Eletrônico Sistema de Registro de Preços nº. _____.

1.2 A especificação técnica do objeto encontra-se descrita no Anexo I do Termo de Referência.

CLÁUSULA SEGUNDA – DA FUNDAMENTAÇÃO LEGAL

2.1 A presente contratação tem como fundamentação legal a Lei nº. 8.666, de 21 de junho de 1993; a Lei nº. 10.520, de 17 de julho de 2002; a Lei Complementar nº. 123, de 14 de dezembro de 2006; o artigo 10, § 7º, do Decreto-Lei nº. 200, de 25 de fevereiro de 1967; o Decreto nº. 3.931, de 19 de setembro de 2001; o Decreto nº. 6.204, de 5 de setembro de 2007; o Decreto nº. 7.174, de 12 de maio de 2010; o Decreto nº. 7.892, de 23 de janeiro de 2013; o Decreto nº. 8.184, de 17 de janeiro de 2014; as Notas Técnicas da Secretaria de Fiscalização de Tecnologia da Informação do Tribunal de Contas da União (SEFTI/TCU) nº. 1/2008 e nº. 2/2008; e a Instrução Normativa da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão (SLTI/MPOG) nº. 4, de 11 de setembro de 2014.

CLÁUSULA TERCEIRA – DO VALOR

3.1 O valor da presente contratação para o período de 12 (doze) meses é de R$ _____ (_____), conforme tabela abaixo:

LOTE	ITEM	DESCRIÇÃO DOS ITENS	Quantidade	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
1 - Solução de Proteção de Perímetro Físico	1	MÓDULO DE CONTROLE DE PERÍMETRO FÍSICO	2	HARDWARE	R$ _____	R$ _____
1 - Solução de Proteção de Perímetro Físico	2	MÓDULO DE PROTEÇÃO À USUÁRIOS E SERVIDORES CRÍTICOS	1200	LICENÇA	R$ _____	R$ _____
1 - Solução de Proteção de Perímetro Físico	3	MÓDULO DE INTELIGÊNCIA NO COMBATE À AMEAÇAS	1	LICENÇA	R$ _____	R$ _____
1 - Solução de Proteção de Perímetro Físico	4	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO DE PERÍMETRO FÍSICO	1	SERVIÇO	R$ _____	R$ _____
2 - Solução de Proteção de Perímetro Virtual	5	MÓDULO DE CONTROLE DE PERÍMETRO VIRTUAL	4	SOFTWARE	R$ _____	R$ _____

2 - Solução de Proteção de Perímetro Virtual	6	MÓDULO DE GERÊNCIA CENTRALIZADO	1	SOFWARE	R$ _____	R$ _____
2 - Solução de Proteção de Perímetro Virtual	7	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO E GERÊNCIA CENTRALIZADA DO PERIMETRO VIRTUAL	1	SERVIÇO	R$ _____	R$ _____
						R$ _____

CLÁUSULA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA

4.1 Para atender aos compromissos decorrentes da execução, os recursos orçamentários estão adequados com _____:

- Funcional Programática: _____;
- Natureza da Despesa: _____;
- Fonte de Recursos: _____;
- Nota de Empenho nº. _____.

CLÁUSULA QUINTA – DO PRAZO DE VIGÊNCIA E DE EXECUÇÃO

5.1 O prazo de vigência do Contrato para os itens 1, 2, 3, 5 e 6 da tabela constante na Cláusula Terceira, objeto da contratação, é de 48 (quarenta e oito) meses, contados da data de sua assinatura, podendo ser renovado.

5.2 O prazo de vigência do Contrato para os itens 4 e 7 da tabela constante na Cláusula Terceira, objeto da contratação, é de 48 (quarenta e oito) meses, contados a partir da data de assinatura, podendo ser renovado por mais 12 (doze) meses, tendo como fundamento o que dispõe o inciso II, artigo 57 da Lei nº. 8.666/1993.

5.3 Os itens 1, 2, 3, 5 e 6 da tabela constante na Cláusula Terceira, objeto da contratação, deverão ser solicitados por meio de ordem de serviço cuja execução deve ser feita em até 60 (sessenta) dias.

5.4 Os itens 4 e 7 da tabela constante na Cláusula Terceira, objeto da contratação, referem-se à prestação de serviço técnico que deverá ser feito imediatamente após abertura da ordem de serviço específica para esses itens.

CLÁUSULA SEXTA – DO PAGAMENTO

6.1 Os valores referentes aos serviços devem ser pagos por demanda, de acordo com a emissão de ordem de serviço com o aceite definitivo realizado.

6.2 O pagamento será efetuado à **CONTRATADA**, no prazo de até 30 (trinta) dias úteis contados da data da emissão da apresentação da fatura ou nota fiscal.

6.3 A nota fiscal/fatura não poderá ser apresentada antes solicitação do gestor, que atestará os serviços.

6.4 Nos casos de eventuais atrasos de pagamento, desde que a **CONTRATADA** não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela **CONTRATANTE**, entre a data do vencimento e o efetivo adimplemento da parcela, é calculada mediante a aplicação da seguinte fórmula:

EM = I x N x VP

Na qual:
I = (TX/100)/365
Onde: EM = Encargos moratórios.
I = Índice de atualização financeira.
TX = Taxa de Juro Anual.
N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento.
VP = Valor da parcela em atraso; = 0,00016438, assim apurado:
I = (i/100)/365; onde i = taxa percentual anual no valor de 6%.

6.5 No caso de incorreção dos documentos apresentados, inclusive na nota fiscal/fatura, serão os mesmos restituídos à **CONTRATADA** para correções necessárias, não respondendo a **CONTRATANTE** por quaisquer encargos resultantes de atrasos na liquidação dos pagamentos correspondentes.

6.6 Caso a **CONTRATADA** seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresa de Pequeno Porte (SIMPLES), deverá apresentar juntamente com a Nota Fiscal/Fatura a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

6.7 Constatada a irregularidade fiscal por meio de consulta on-line ao Sistema de Cadastramento Unificado de Fornecedores (SICAF), ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou a documentação mencionada no artigo 29 da Lei nº. 8.666/1993, a **CONTRATADA** será advertida, por escrito, para que no prazo de até 5 (cinco) dias úteis, apresente a regularização fiscal junto ao SICAF, sob pena de rescisão do Contrato.

6.8 O prazo para regularização referido no item 6.7 poderá ser prorrogado desde que a justificativa apresentada seja aceita pela **CONTRATANTE**.

6.9 Demais exigências para o cronograma de desembolso estão previstas no item 20 do Termo de Referência.

CLÁUSULA SÉTIMA – DEVERES E RESPONSABILIDADES DA CONTRATADA

7.1 Cumprir fielmente as obrigações assumidas em Contrato, observando as definições técnicas do Termo de Referência, entregando os serviços no prazo estipulado, na forma e nas condições pactuadas.

7.2 Manter-se, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do Contrato.

7.3 Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços a serem executados não podendo invocar posteriormente desconhecimento para cobrança de serviços extras.

7.4 Submeter à aprovação da **CONTRATANTE** qualquer alteração que se tornar essencial à continuação da execução ou prestação dos serviços.

7.5 Aceitar, nas mesmas condições contratuais, os acréscimos ou as supressões que se fizerem no objeto contratual, até 25% (vinte e cinco inteiros por cento) do seu valor inicial.

7.6 Refazer os serviços nos quais se verifiquem danos ou qualquer defeito nos materiais e sistemas utilizados, no prazo máximo de 5 (cinco) dias úteis, contados da notificação que lhe for entregue oficialmente, sob pena sofrer sanções por inexecução contratual.

7.7 Comunicar à **CONTRATANTE**, por escrito, no prazo máximo de 5 (cinco) dias úteis que antecedem o prazo de vencimento das entregas, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos.

7.8 Obter todo e qualquer tipo de licença junto aos órgãos fiscalizadores para o perfeito e efetivo fornecimento da solução ofertada, sem ônus adicional para a **CONTRATANTE**.

7.9 Arcar com todas as despesas referentes à prestação dos serviços, tais como frete, seguro, taxas, transportes e embalagens, bem como os encargos trabalhistas,

previdenciários, comerciais e salários dos seus empregados, para entrega do serviço no prazo estipulado.

7.10 Cumprir com as normas de segurança e medicina do trabalho durante possível estadia dos seus profissionais nas instalações da **CONTRATANTE**.

7.11 Assumir todas as responsabilidades e tomar as medidas necessárias ao atendimento dos seus empregados, acidentados ou acometidos de mal súbito, quando em serviço, assegurando-lhes o cumprimento a todas as determinações trabalhistas e previdenciárias cabíveis e assumindo, ainda, as responsabilidades civis, penais, criminais e demais sanções legais decorrentes do eventual descumprimento destas.

7.12 Cumprir, além dos postulados legais vigentes de âmbito, federal, estadual, distrital e/ou municipal, as normas de segurança do **CONTRATANTE**, inclusive quanto à prevenção de incêndios e as de Segurança e Medicina do Trabalho.

7.13 Emitir Comunicado de Acidente de Trabalho (CAT), em formulário próprio do Instituto Nacional do Seguro Social (INSS), em caso de eventual ocorrência de acidente com seus empregados nas dependências do **CONTRATANTE**, apresentando cópia do mesmo à fiscalização do Contrato.

7.14 Responder pelos danos, decorrentes de sua culpa ou dolo, causados diretamente à Administração ou a terceiros, não excluindo ou reduzindo esta responsabilidade à fiscalização e acompanhamento por parte do **CONTRATANTE**.

7.15 Arcar com os prejuízos e danos causados pelos seus funcionários aos bens móveis, imóveis, sistemas, utensílios, mobiliário etc. da **CONTRATANTE**, substituindo-os após comunicação formal do fiscal do Contrato, por materiais ou bens idênticos ou recuperados quando possível, deixando-os em perfeito estado de conservação ou funcionamento no prazo máximo de 72 (setenta e duas) horas.

7.16 Agendar, pelo telefone (61) 2029-6428, a entrada de sistemas ou materiais no ambiente da **CONTRATANTE**, dentro do horário das 9h às 12h e das 14h às 18h, de segunda a sexta-feira, em dias úteis, a fim de que seja designado pessoal técnico da **CONTRATANTE** para a verificação e acompanhamento.

7.17 Manter seus funcionários ou representantes credenciados devidamente identificados quando da execução de qualquer serviço nas dependências da

CONTRATANTE referente ao objeto contratado observando as normas de segurança (interna e de conduta).

7.18 Atender às solicitações emitidas pela gestão do Contrato quanto ao fornecimento de informações e/ou documentação.

7.19 Manter o mais rigoroso sigilo sobre quaisquer dados, informações, documentos e especificações que a ela venham a ser confiados ou que venha a ter acesso em razão da execução dos serviços, não podendo, sob qualquer pretexto, revelá-los, divulgá-los, reproduzi-los ou deles dar conhecimento a quaisquer terceiros.

7.20 Indicar o preposto para, em todas as questões relativas ao cumprimento dos serviços, representar a **CONTRATADA**, de forma a garantir a presteza e a agilidade necessária ao processo decisório. O preposto será o responsável da **CONTRATADA** pela execução do Contrato, e deverá e reportar-se à **CONTRATADA**, indicando seu cargo, endereço com CEP, número de telefone residencial e celular, número do fac-símile e endereço eletrônico.

7.21 Emitir relatório de serviços, depois de concluída qualquer manutenção, em que constem informações referentes ao serviço realizado, número do chamado, data e hora do chamado, e hora do início e do término do atendimento.

7.22 O relatório deverá ser acompanhado, ainda, de eventual comunicação de novas versões de *software*, *patches* de atualização e vulnerabilidades encontradas nos produtos.

CLÁUSULA OITAVA – DEVERES E RESPONSABILIDADES DA CONTRATANTE

8.1 Prestar informações e esclarecimentos que venham a ser solicitados pela **CONTRATADA**.

8.2 Acompanhar e fiscalizar o andamento dos serviços de assistência técnica, devendo para tanto nomear um fiscal de Contrato e um gestor, ou uma comissão, que responsabilizar-se-ão pelo acompanhamento dos serviços, conferência e atesto das faturas e cumprimento das demais exigências previstas no Contrato.

8.3 Observar para que, durante a vigência do Contrato, sejam mantidas, pela **CONTRATADA**, as compatibilidades com as obrigações assumidas e todas as condições e qualificações exigidas para a pactuação.

8.4 Comunicar formal, circunstanciada e tempestivamente à **CONTRATADA**, qualquer anormalidade ocorrida durante a execução do Contrato.

8.5 Promover os pagamentos na forma pactuada.

8.6 Receber e atestar as faturas, quando do aceite definitivo, conforme condições e especificações constantes do Termo de Referência.

8.7 Proceder à consulta ao SICAF antes de efetuar o pagamento.

8.8 Indicar um técnico para acompanhar a entrega dos produtos.

8.9 Permitir acesso dos profissionais da **CONTRATADA** às suas dependências quando da prestação dos serviços.

8.10 Receber e conferir a solução entregue, procedendo à imediata devolução daquela que se encontrar com especificação em desacordo do exigido no Contrato.

8.11 Solicitar assistência técnica quando da constatação de algum defeito na operacionalização da Solução.

8.12 Conferir toda a documentação técnica gerada e apresentada durante a execução dos serviços, efetuando o seu atesto quando a mesma estiver em conformidade com os padrões de informação e qualidade exigidos.

8.13 Exigir, uma vez comprovada a necessidade, o imediato afastamento do ambiente da **CONTRATANTE**, de qualquer profissional e/ou preposto da **CONTRATADA** que, por justas razões, vier a desmerecer a confiança, embarace a fiscalização ou, ainda, que venha a se conduzir de modo inconveniente ou incompatível com o exercício das funções que lhe forem delegadas.

8.14 Solicitar ao gestor do Contrato as decisões e providências que ultrapassem a sua competência, em tempo hábil, para adequada adoção das medidas julgadas cabíveis, quando a contratada não cumprir com as obrigações avençadas.

CLÁUSULA NONA – DOS ACRÉSCIMOS E SUPRESSÕES

9.1 A **CONTRATADA** e **CONTRATANTE** aceitarão acréscimos ou supressões no(s) serviço(s) objeto do presente Contrato, em até 25% (vinte e cinco inteiros por cento) do valor do Contrato, de acordo com o definido no artigo 65 da Lei nº. 8.666/1993, via Termo Aditivo.

CLÁUSULA DÉCIMA – DA FISCALIZAÇÃO DO CONTRATO

10.1 Para o acompanhamento e a fiscalização da execução do Contrato serão

designados representantes da **CONTRATANTE**, nos termos do artigo 67 da Lei nº. 8.666/1993 e da Instrução Normativa SLTI/MPOG nº. 4/2014, que se responsabilizarão pelo registro de todas as ocorrências relacionadas com a execução e determinarão o que for necessário à regularização de falhas ou defeitos observados.

10.2 A fiscalização de que trata o item anterior não exclui nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios, e, na ocorrência desta, não implica em corresponsabilidade da **CONTRATANTE** ou de seus agentes, em conformidade com o artigo 70 da Lei nº. 8.666/1993.

10.3 O Contrato será acompanhado e fiscalizado pelos seguintes agentes da **CONTRATANTE**:

10.3.1 Fiscal técnico, fiscal administrativo, fiscal requisitante, gestor do Contrato.

10.4 O Contrato será acompanhado por empregados da **CONTRATANTE**, com o objetivo de garantir a adequada prestação dos serviços e o fornecimento dos bens que compõem a Solução de Tecnologia da Informação durante todo o período de sua execução e compreende, nos termos da Instrução Normativa SLTI/MPOG nº. 4/2010, as seguintes tarefas:

10.5 Realização de reunião inicial, convocada pelo seu gestor, com a participação dos fiscais, da **CONTRATADA**, e demais intervenientes por ele identificados, para apresentação do preposto e dos serviços oferecidos pela **CONTRATADA**; breve explanação sobre o portal de acesso à sua base de conhecimento; entrega do termo de compromisso e do termo de ciência; esclarecimentos relativos a questões operacionais, administrativas e de gerenciamento do Contrato, dentre outros assuntos que forem relevantes para dar início à sua execução;

10.6 Encaminhamento formal de Autorização de Início dos Serviços pelo gestor do Contrato ao preposto da **CONTRATADA**;

10.7 Monitoramento da execução, pelos fiscais e pelo gestor do Contrato;

10.8 Confecção e assinatura do Termo de Recebimento Provisório, cujo modelo consta do Anexo III do Termo de Referência, a cargo do fiscal técnico do Contrato;

10.9 Avaliação da qualidade dos serviços realizados e justificativas, de acordo com os critérios de aceitação definidos em Contrato, a cargo dos fiscais técnico e requisitante

do Contrato;

10.10 Identificação de não conformidade com os termos contratuais, a cargo dos fiscais técnico e requisitante do Contrato;

10.11 Verificação de aderência aos termos contratuais, a cargo do fiscal administrativo do Contrato;

10.12 Verificação da manutenção das condições classificatórias referentes à habilitação técnica, a cargo dos fiscais administrativo e técnico do Contrato;

10.13 Encaminhamento das demandas de correção à **CONTRATADA**, a cargo do gestor do Contrato;

10.14 Encaminhamento de indicação de sanções por parte do gestor do Contrato para a área administrativa;

10.15 Confecção e assinatura do Termo de Recebimento Definitivo, para fins de encaminhamento para pagamento, cujo modelo consta do Anexo VI do Termo de Referência, a cargo do gestor e do fiscal requisitante do Contrato;

10.16 Verificação das regularidades fiscais, trabalhistas e previdenciárias para fins de pagamento, a cargo do fiscal administrativo do Contrato;

10.17 Verificação da manutenção da necessidade, economicidade e oportunidade da contratação, a cargo do fiscal requisitante do Contrato;

10.18 Verificação de manutenção das condições elencadas no Plano de Sustentação, a cargo dos fiscais técnico e requisitante do Contrato;

10.19 Encaminhamento à área administrativa de eventuais pedidos de modificação contratual, a cargo do gestor do Contrato; e

10.20 Manutenção do histórico de gerenciamento do Contrato, contendo registros formais de todas as ocorrências positivas e negativas da execução do Contrato, por ordem histórica, a cargo do gestor do Contrato;

10.21 Transição contratual, quando aplicável, e encerramento do Contrato, que deverá observar o Plano de Sustentação;

10.22 No caso de prorrogação contratual, o gestor do Contrato deverá, com base na documentação contida no histórico de gerenciamento do Contrato e nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, encaminhar à área administrativa, com pelo menos 60 (sessenta) dias de antecedência do término do

Contrato, documentação explicitando os motivos para a prorrogação; e

10.23 No caso dos demais aditamentos contratuais, o gestor do Contrato deverá encaminhar, à área administrativa, documentação explicitando os motivos para tal aditamento.

10.24 A gestão e fiscalização deste Contrato pela **CONTRATANTE** não excluem nem reduzem a responsabilidade da **CONTRATADA** pelo cumprimento das obrigações decorrentes deste instrumento.

10.25 O modelo de prestação de serviço/fornecimento de bens encontra-se descrito no item 3 do Termo de Referência.

CLÁUSULA DÉCIMA PRIMEIRA – DO MÉTODO DE AVALIAÇÃO DE CONFORMIDADE DOS PRODUTOS E SERVIÇOS E NOS NÍVEIS DE SERVIÇO

11.1 RECEBIMENTO PROVISÓRIO

11.1.1 O **CONTRATANTE** realizará o recebimento provisório do(s) equipamento(s), do(s) *software*(s) e serviço(s) no momento da entrega;

11.1.1.1 Todos os equipamentos/serviços deverão ser entregues/prestados em Brasília, ou em local previamente acordado em reunião de instrução, no horário de funcionamento da **CONTRATANTE**;

11.1.2 A equipe técnica da Superintendência de Tecnologia da Informação (SUPTI) da **CONTRATANTE** realizará inspeção técnica dos equipamentos para verificação da sua integridade física e aderência às especificações constantes do Edital;

11.1.3 Após a inspeção técnica nos equipamentos e verificando que estes estão em perfeitas condições, a equipe técnica deverá emitir o Termo de Recebimento Provisório, a ser entregue ao preposto ou representante da **CONTRATADA**. Este documento garante à **CONTRATADA** que os itens constantes da ordem de serviço foram entregues à **CONTRATANTE** para avaliação de sua qualidade e conformidade;

11.1.4 Os equipamentos deverão ser entregues em perfeito estado de funcionamento, sem marcas, amassados, arranhões e/ou outros problemas físicos;

11.1.5 O(s) equipamento(s), acessório(s) e/ou componente(s) entregue(s) que apresentar(em) inconformidade(s), defeito por transporte e/ou por processo fabril, deverá(ão) ser substituído(s) pela **CONTRATADA**, em um prazo de 15 (quinze) dias corridos, contados a partir da notificação pela **CONTRATANTE**.

11.2 RECEBIMENTO DEFINITIVO

11.2.1 Verificando-se a conformidade dos itens da ordem de serviço entregues pela **CONTRATADA**, a **CONTRATANTE** deve verificar se a execução da ordem de serviço se deu de forma aderente aos termos contratuais. Estando o processo aderente, a **CONTRATANTE** emitirá o Termo de Recebimento Definitivo, que será entregue à **CONTRATADA**;

11.2.2 Caso seja verificada a não aderência aos termos contratuais, a **CONTRATANTE** deverá indicar os termos que não estão aderentes ao Contrato e deverá encaminhar a sua área administrativa para sanções cabíveis.

11.3 A metodologia de avaliação do nível de serviço está prevista no item 9 do Termo de Referência.

CLÁUSULA DÉCIMA SEGUNDA – DA SUBCONTRATAÇÃO

12.1 Será permitida a subcontratação para a execução dos serviços e fornecimento de bens somente de empresas pertencentes à rede autorizada do fabricante dos sistemas.

12.2 Será observado o limite de subcontratação em 30% (trinta por cento) do valor do lote.

CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTE

13.1 No que não contrariar o artigo 5º do Decreto nº. 2.271/1997, o reajuste se regerá da seguinte forma:

13.1.1 O preço do Contrato é fixo e irreajustável para os itens 1, 2, 3, 5 e 6 da tabela constante na Cláusula Terceira.

13.1.2 O preço do Contrato poderá ser reajustado para os itens 4 e 7 da tabela constante na Cláusula Terceira, caso haja renovação contratual, após o período de 48 (quarenta e oito) meses.

13.2 Na situação de reajuste, esse deverá ser feito utilizando o Índice Nacional de Preços ao Consumidor Amplo (IPCA), dos 12 (doze) últimos meses contados 2 (dois) meses antes do vencimento do Contrato, como índice de reajuste, ou outro que venha a substituí-lo, conforme artigo 19, inciso XXII, da Instrução Normativa SLTI/MPOG nº. 2/2008, obedecida a legislação vigente.

CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO

14.1 O presente Contrato poderá ser rescindido, na forma e na ocorrência de qualquer das hipóteses previstas nos artigos 77 a 80 da Lei nº. 8.666/1993. Neste caso, deverá ser formalmente motivado, nos autos do processo, assegurados o contraditório e a ampla defesa.

CLÁUSULA DÉCIMA QUINTA – DAS SANÇÕES ADMINISTRATIVAS

15.1 Pela inexecução total ou parcial das obrigações assumidas, garantidas a prévia defesa, a Administração poderá aplicar à **CONTRATADA**, as sanções previstas em Contrato e no Termo de Referência, conforme descrição a seguir:

15.2 Advertência, nos termos da Lei;

15.3 Multas conforme descrição a seguir:

15.3.1 O atraso injustificado no cumprimento dos prazos assumidos em Contrato implicará em multa de 0,33% (trinta e três centésimos por cento) por dia útil após a data fixada, calculada sobre o valor total da fatura a ser paga, até o limite máximo de 10% (dez por cento);

15.3.2 Na hipótese mencionada no subitem anterior, a atraso injustificado ou cuja justificativa tenha sido rejeitada pela **CONTRATANTE**, superior a 30 (trinta) dias úteis, caracterizará o descumprimento das obrigações, total ou parcial, conforme o caso, sendo passível de punição com advertência e multa de 20% (vinte por cento) sobre o valor total do Contrato, assim como configurada a inexecução do Contrato, podendo a **CONTRATANTE** rescindi-lo unilateralmente;

15.3.3 A inobservância dos prazos de atendimento dos chamados relativos à Garantia e Assistência, conforme disposto no Acordo de Nível de Serviço constante do subitem 9 do Termo de Referência, implicará à **CONTRATADA**, além das penalidades previstas no Anexo IV do Termo de Referência, a cominação de rescisão unilateral pela Administração Pública, do Contrato firmado, por inexecução contratual;

15.3.4 A rescisão a que se refere a alínea anterior será precedida de punição com multa de 20% (vinte por cento) sobre o valor total do Contrato;

15.3.5 As multas e glosas porventura aplicadas serão descontadas dos pagamentos devidos pelo **CONTRATANTE**, da garantia do Contrato, ou cobradas diretamente da **CONTRATADA**, amigável ou judicialmente, e poderão ser aplicadas cumulativamente com as demais sanções previstas.

15.4 Suspensão temporária de participação em licitações e impedimento de contratar com a União;

15.5 Declaração de inidoneidade para licitar ou contratar com a Administração Pública.

15.6 Aquele que deixar de entregar os documentos, ou apresentar documentação exigida para o certame falsa; ensejar o retardamento da execução do objeto contratual; não mantiver a proposta; falhar ou fraudar a execução do Contrato; comportar-se de modo inidôneo; fazer declaração falsa ou cometer fraude fiscal ficará impedido de licitar e contratar com a União, e será descredenciado do SICAF pelo prazo de até 5 (cinco) anos, sem prejuízo da multas previstas em Edital e no Contrato e das demais cominações legais, conforme disposto no artigo 28 do Decreto nº. 5.450/2005.

15.7 Das penalidades aplicadas caberá recurso, no prazo de 5 (cinco) dias úteis, observados o procedimento estabelecido no artigo 109 da Lei nº. 8.666/1993, dirigido à autoridade superior por intermédio da que praticou o ato recorrido, a qual poderá reconsiderar sua decisão.

15.8 Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá a **CONTRATADA** pela sua diferença que será descontada dos pagamentos eventualmente devidos pela **CONTRATANTE** ou cobrada judicialmente.

15.9 As penalidades serão obrigatoriamente registradas no SICAF e, no caso de suspensão de licitar, a **CONTRATADA** deverá ser descredenciada por igual período, sem prejuízo das multas previstas no Termo de Referência e das demais cominações legais.

15.10 As multas aplicadas deverão ser recolhidas no prazo de 5 (cinco) dias, a contar da data da notificação, podendo a Administração descontar o seu valor da nota fiscal ou documento de cobrança, independente de notificação, por ocasião de seu pagamento, ou cobrá-las judicialmente, segundo da Lei nº. 6.830/1980, com os encargos correspondentes.

CLÁUSULA DÉCIMA SEXTA – DA GARANTIA

16.1 A **CONTRATADA** deverá apresentar, no prazo de até 10 (dez) dias úteis, prorrogáveis por igual período, a critério da **CONTRATANTE**, contados da data da assinatura do Contrato, comprovante de prestação de garantia, no valor correspondente

a 5% (cinco por cento) do valor global do Contrato, devendo ser renovada a cada prorrogação efetiva no Contrato, nos moldes do artigo 56 da Lei nº. 8.666, de 1993, sob pena de aplicação de sanções previstas neste Contrato e no Edital.

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

16.2.1 prejuízos advindos do não cumprimento do objeto do Contrato;

16.2.2 prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do Contrato;

16.2.3 multas moratórias e punitivas aplicadas pela Administração à **CONTRATADA**;

16.2.4 obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela **CONTRATADA**, quando couber.

16.3 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item 16.2, observada a legislação que rege a matéria.

16.4 A garantia em dinheiro deverá ser efetuada na Caixa Econômica Federal em conta específica com correção monetária, em favor do **CONTRATANTE**.

16.5 A inobservância do prazo fixado para apresentação da garantia acarretará a aplicação de multa de 0,07% (sete centésimos por cento) do valor do Contrato por dia de atraso, observado o máximo de 2% (dois por cento).

16.6 O atraso superior a 25 (vinte e cinco) dias autoriza a Administração a promover a rescisão do Contrato por descumprimento ou cumprimento irregular de suas Cláusulas.

16.7 O garantidor não é parte para figurar em processo administrativo instaurado pelo **CONTRATANTE** com o objetivo de apurar prejuízos e/ou aplicar sanções à **CONTRATADA**.

16.8 A garantia será considerada extinta:

16.8.1 Com a devolução da apólice, fiança bancária 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;

16.8.2 O prazo de 90 (noventa) dias após o término da vigência do Contrato, que

poderá ser estendido em caso de ocorrência de sinistros.

CLÁUSULA DÉCIMA SÉTIMA – DA PUBLICAÇÃO

17.1 A **CONTRATANTE** providenciará a publicação deste instrumento, por extrato, nos termos do parágrafo único do artigo 61, da Lei nº. 8.666/1993.

CLÁUSULA DÉCIMA OITAVA - DO ANTINEPOTISMO E DA OBSERVÂNCIA AO REGRAMENTO ÉTICO E DE INTEGRIDADE DA CONTRATANTE

18.1 Fica vedada à **CONTRATADA** alocar, para prestação dos serviços que constituem o objeto do presente contrato, familiar de agente público que neste exerça cargo em comissão ou função de confiança do **CONTRATANTE**.

18.2 Considera-se familiar, nos termos do artigo 2º, inciso III, do Decreto nº. 7.203, de 4 de junho de 2010, o cônjuge, o companheiro ou o parente em linha reta ou colateral, por consanguinidade ou afinidade, até o terceiro grau.

18.3 A **CONTRATADA** deverá observar o Código de Ética da **CONTRATANTE**, que está disponível no sítio da **CONTRATANTE**, no seguinte endereço: http://www.valec.gov.br/ComissaoDeEtica.php.

18.4 Nos termos do que dispõe a Lei nº. 12.846, de 1º de agosto de 2013, regulamentada pelo Decreto nº. 8.420, de 18 de março de 2015, que tratam da responsabilidade administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e o item XXIV do Anexo do Decreto nº. 1.171, de 22 de junho de 1994, que tipifica o Agente Público no âmbito do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, a **CONTRATADA** deverá:

18.4.1 Adotar conduta compatível com o Código de Ética da **CONTRATANTE** e orientar seus funcionários, prepostos e subcontratados que desempenhem os serviços contratados, a observância do regramento ético estabelecido pela **CONTRATADA**;

18.4.2 Cumprir, rigorosamente, o conjunto de mecanismos e procedimentos de integridade estabelecido pela **CONTRATANTE** e na legislação de regência, associados ao objeto contratado;

18.4.3 Comunicar à **CONTRATANTE** e às autoridades competentes eventuais práticas ilícitas ocorridas na vigência deste Contrato, que comprometam as condutas éticas e de integridade, bem como colaborar com as investigações e, se for o caso,

adotar medidas para sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a pessoa, a administração pública, nacional e estrangeira, mitigando as falhas cometidas

CLÁUSULA DÉCIMA NONA – DISPOSIÇÕES GERAIS,

19.1 A **CONTRATANTE** rejeitará, no todo ou em parte, o fornecimento executado em desacordo com o objeto contratado.

19.2 Os empregados da **CONTRATADA** não terão nenhum vínculo empregatício com a **CONTRATANTE**.

19.3 Os casos não abordados serão definidos pela fiscalização da **CONTRATANTE**, de maneira a manter o padrão de qualidade previsto para os serviços em questão.

19.4 Na hipótese de divergência das disposições entre o Termo de Referência e o Contrato, prevalecerão as disposições do Termo de Referência e seus Anexos.

19.5 Fazem parte integrante do presente instrumento, independentemente de transcrição, o Termo de Referência e seus Anexos, além da Proposta de Preços da **CONTRATADA** e seus Anexos, devidamente autuados no Processo nº. 51402.180668/2017-96.

CLÁUSULA VIGÉSIMA – DO FORO

20.1 O foro competente, eleito pelas partes, é o da Justiça Federal da cidade de Brasília (Seção Judiciária do Distrito Federal), com expressa renúncia de qualquer outro, por mais privilegiado que seja para dirimir quaisquer dúvidas decorrentes do presente Contrato.

E, por estarem assim justas e acordadas, as partes assinam o presente instrumento em 3 (três) vias de igual teor e para um só efeito, na presença das testemunhas abaixo.

Brasília, de de 2018.

VALEC - ENGENHARIA, CONSTRUÇÕES E FERROVIAS S. A.

MÁRCIO GUIMARÃES DE AQUINO
Diretor de Planejamento

MÁRIO MONDOLFO
Diretor-Presidente

XXXXX
XXXXXX

TESTEMUNHAS:

NOME: CPF:

NOME: CPF:

ANEXO III

ATA DE REGISTRO DE PREÇOS nº. ___/2018 - VALEC

PROCESSO nº. 51402.180668/2017-96
PREGÃO ELETRÔNICO SISTEMA DE REGISTRO DE PREÇO (SRP) nº ___/2018

VALEC – ENGENHARIA, CONSTRUÇÕES E FERROVIAS S. A., inscrita no CNPJ/MF sob o nº. 42.150.664/0001-87, situada no Setor de Autarquias Sul (SAUS), Quadra 1, Bloco "G", Lotes 3 e 5, Asa Sul, Brasília (DF), CEP 70.070-010, representada pelo seu Diretor-Presidente, **MÁRIO MONDOLFO**, brasileiro, casado, engenheiro civil, portador da cédula de identidade nº. 6.578.384-0 SSP/SP, inscrito no CPF sob o nº. 913.529.248-20, residente e domiciliado em São Paulo (SP), e por seu Diretor de Planejamento, **MÁRCIO GUIMARÃES DE AQUINO**, brasileiro, casado, administrador, portador da carteira de identidade nº. 1.561.673-SSP/DF, inscrito no CPF sob o n°. 631.403.497-34, residente e domiciliado na cidade de Brasília (DF), nos termos da Lei nº. 8.666, de 21 de junho de 1993, da Lei nº. 10.520, de 17 de julho de 2002, e dos Decretos nº. 5.540, de 31 de maio de 2005 e nº. 7.892, de 23 de janeiro de 2013, e demais normas legais aplicáveis, em face da classificação da proposta apresentada no Pregão Eletrônico SRP nº. ___/2018, **RESOLVE** registrar o preço ofertado por _____, inscrito no CNPJ/MF sob o nº. _____, com sede no endereço _____, doravante denominado **CONTRATADA**, neste ato representada por seu representante _____, portador da carteira de identidade nº. _____, inscrito no CPF sob o nº. _____, conforme abaixo:

- Contratação de empresa para a aquisição de plataforma de segurança com funcionalidade de proteção à rede, usuários/servidores críticos e inteligência no combate a ameaças, incluindo o fornecimento de equipamentos e *softwares* integrados em forma de *appliance* e/ou *software appliance* (módulo virtual) quando especificado, serviços de instalação e configuração, suporte técnico e garantia e transferência de conhecimento, mediante Sistema Registro de Preços, conforme itens constantes na tabela abaixo:

LOTE	ITEM	DESCRIÇÃO DOS ITENS	Quantidade	UNIDADE	VALOR UNITÁRIO	VALOR TOTAL
1 - Solução de Proteção de Perímetro Físico	1	MÓDULO DE CONTROLE DE PERÍMETRO FÍSICO	2	HARDWARE	R$ _____	R$ _____

1 - Solução de Proteção de Perímetro Físico	2	MÓDULO DE PROTEÇÃO À USUÁRIOS E SERVIDORES CRÍTICOS	1200	LICENÇA	R$ _____	R$ _____
1 - Solução de Proteção de Perímetro Físico	3	MÓDULO DE INTELIGÊNCIA NO COMBATE À AMEAÇAS	1	LICENÇA	R$ _____	R$ _____
1 - Solução de Proteção de Perímetro Físico	4	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO DE PERÍMETRO FÍSICO	1	SERVIÇO	R$ _____	R$ _____
2 - Solução de Proteção de Perímetro Virtual	5	MÓDULO DE CONTROLE DE PERÍMETRO VIRTUAL	4	SOFTWARE	R$ _____	R$ _____
2 - Solução de Proteção de Perímetro Virtual	6	MÓDULO DE GERÊNCIA CENTRALIZADO	1	SOFWARE	R$ _____	R$ _____
2 - Solução de Proteção de Perímetro Virtual	7	SUPORTE TÉCNICO DOS MÓDULOS DE PROTEÇÃO E GERÊNCIA CENTRALIZADA DO PERIMETRO VIRTUAL	1	SERVIÇO	R$ _____	R$ _____
						R$ _____

1.1. Esta Ata de Registro de Preços tem vigência de 12 (doze) meses, contados da data de sua assinatura.

As especificações técnicas constantes do Edital do Pregão Eletrônico nº. ___/2018 integram esta Ata de Registro de Preços, independentemente de transcrição.

A presente Ata, após lida e achada conforme, é assinada pelos representantes legais da **VALEC - ENGENHARIA, CONSTRUÇÕES E FERROVIAS S. A.** e **_____.**

Brasília, _____ de _____ de 2018.

VALEC – ENGENHARIA, CONSTRUÇÕES E FERROVIAS S. A.

MÁRCIO GUIMARÃES DE AQUINO
Diretor de Planejamento

MÁRIO MONDOLFO
Diretor-Presidente

_____

_____

TESTEMUNHAS:

Nome: CPF:

Nome: CPF:

ANEXO I

Em conformidade com o disposto nos artigos 10 a 13 do Decreto nº. 7.892/2013, que regulamenta o Sistema de Registro de Preços previsto no artigo 15 da Lei nº. 8.666, de 21 de junho de 1993, ficam incluídos no cadastro de reserva, com o preço idêntico ao registrado pelo vencedor do Pregão Eletrônico nº. ___/2018, os seguintes fornecedores:

FORNECEDOR	CNPJ	LOTE/ITEM

VALEC – ENGENHARIA, CONSTRUÇÕES E FERROVIAS S. A.

MÁRCIO GUIMARÃES DE AQUINO
Diretor de Planejamento

MÁRIO MONDOLFO
Diretor-Presidente

_____

_____

TESTEMUNHAS:

Nome: CPF:

Nome: CPF:

TERMO DE ENCERRAMENTO

Este volume do **Edital nº 2/2018** de **Pregão Eletrônico** possui XX (XXXX) folhas numericamente ordenadas**.**

Brasília/DF, XX de fevereiro de 2018.

Flávia Carneiro de Oliveira
Superintendente de Licitações e Contratos