# TERMO DE REFERÊNCIA - TR

## 1 DO OBJETO

1.1 Aquisição de Solução de Segurança NGFW com Subscrição e Produto para o **IBAMA - INSTITUTO BRASILEIRO DO MEIO AMBIENTE E DOS RECURSOS NATURAIS RENOVÁVEIS**, incluindo instalação, capacitação técnica, garantia e suporte, através de **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO.**

## 2 DA JUSTIFICATIVA

2.1 O Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (Ibama) é uma autarquia federal vinculada ao Ministério do Meio Ambiente dotada de personalidade jurídica de direito público, autonomia administrativa e financeira.

2.2 Foi criado em 1989 pelo art. 2º da Lei nº 7.735 e possui a estrutura regimental estabelecida pelo Decreto nº 6.099, de 26 de abril de 2007. Suas principais atribuições são exercer o poder de polícia ambiental federal, executar ações de meio ambiente referentes às atribuições federais de licenciamento ambiental, controle da qualidade ambiental, autorização de uso dos recursos naturais e fiscalização, monitoramento e controle ambiental, e ações supletivas e subsidiárias de competência da União, em conformidade com a legislação vigente.

2.3 Atua sempre em consonância com as diretrizes da Política Nacional de Meio Ambiente, propondo e editando normas e padrões de qualidade ambiental; o zoneamento e a avaliação de impactos ambientais; o licenciamento ambiental federal; a implementação do Cadastro Técnico Federal; a fiscalização ambiental e a aplicação de penalidades administrativas; a geração e a disseminação de informações relativas ao meio ambiente; o monitoramento ambiental, principalmente no que diz respeito à prevenção e ao controle de desmatamentos, queimadas e incêndios florestais; o apoio às emergências ambientais; a execução de programas de educação ambiental; a elaboração do sistema de informação e o estabelecimento de critérios para a gestão do uso dos recursos faunísticos, pesqueiros e florestais, entre outros.

2.4 As principais atividades executadas pelo Ibama são:

2.4.1 Executar o Plano Nacional de Contingência (PNC), em conformidade com o Decreto nº 8.127, de 22 de outubro de 2013;

2.4.2 Coordenar, em parceria com os órgãos estaduais de meio ambiente, a elaboração e implantação dos Planos de Área para o combate à poluição por óleo em águas brasileiras em concentração de portos organizados, instalações portuárias ou plataformas;

2.4.3 Supervisionar a implementação e execução dos planos de prevenção e atendimento a acidentes e emergências ambientais, exigidos no processo de licenciamento ambiental federal;

2.4.4 Coordenar e apoiar as ações de prevenção e resposta a acidentes e emergências ambientais, prioritariamente de eventos oriundos de atividades ou empreendimentos licenciados pelo Ibama;

2.4.5 Participar do comando do incidente unificado em conjunto com órgãos da esfera federal, estadual e municipal no atendimento aos acidentes ambientais de relevância regional e nacional;

2.4.6 Participar, como representante do Ibama, nos colegiados do Sistema de Proteção ao Programa Nuclear Brasileiro (Sipron), inclusive na elaboração de planos de emergências, nos exercícios simulados de emergência nuclear, e nos centros de respostas;

2.4.7 Vistoriar preventivamente as atividades ou empreendimentos com potencial de causar acidentes e emergências ambientais, licenciandos pelo Ibama;

2.4.8 Gerir o Sistema Nacional de Emergências Ambientais (Siema), que é o portal do comunicado inicial de acidente ambiental;

2.4.9 Analisar os requerimentos de emissão da Autorização Ambiental para a realização de Operações Ship-to-Ship, bem como vistorias as empresas autorizadas;

2.4.10 Produzir análises de dados referentes aos acidentes ambientais ocorridos em todo o território brasileiro, visando o planejamento das atividades de suporte às ações de prevenção e atendimento;

2.4.11 Promover, de forma integrada, a capacitação nas ações de atendimento e prevenção de acidentes e emergências ambientais; e

2.4.12 Estabelecer procedimentos para prevenção e atendimento a acidentes e emergências ambientais.

2.5 O IBAMA é de extrema importância para a preservação e manutenção do Meio Ambiente no Brasil. Ele atua de forma eficiente para a preservação de nossas matas, florestas, rios, fauna e recursos naturais diversos. Sem a atuação deste órgão, poderíamos ter um país devastado do ponto de vista ambiental.

2.6 Portanto, para a continuidade das ações supracitadas o Ibama faz uso de diversas soluções na área da tecnologia da informação e comunicação, onde a dependência destes recursos computacionais é fato notório, cuja demanda interna por ampliação dos mesmos é constante, seja pela disponibilização de um novo acesso a rede ou pela necessidade recorrente de incremento de performance, disponibilidade e qualidade dos serviço prestados.

2.7 Um dos segmentos da Tecnologia da Informação, responsável pela parte de comunicações, é denominada por TIC, ou seja, Tecnologia da Informação e Comunicação. É uma expressão que se refere ao papel da comunicação, seja por fios ou sem fio, na moderna tecnologia da informação. Entende-se que esta tecnologia consiste de todos os meios técnicos usados para tratar a informação e auxiliar na comunicação, o que inclui o hardware de computadores, rede, telefonia móvel celular, bem como todo software necessário. Em outras palavras, esta tecnologia consiste em qualquer forma de transmissão de informações e corresponde a todas as tecnologias que interferem e medeiam os processos informacionais e comunicativos dos seres. Ainda, podem ser entendidas como um conjunto de recursos tecnológicos integrados

entre si, que proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica, de ensino e aprendizagem, de fiscalização e proteção ambiental, dentre outras que devidamente aplicadas, garantem a essa Administração manter a excelência nos serviços prestados ao Brasil.

2.8 Atualmente, os sistemas de informação e as redes de computadores têm desempenhado um papel importante na comunicação corporativa, pois é através dessas ferramentas que a comunicação flui sem barreira. Segundo Lévy (1999), novas maneiras de pensar e de conviver estão sendo elaboradas no mundo das telecomunicações e da informática. As relações entre os homens, o trabalho, a própria inteligência dependem, na verdade, da metamorfose incessante de dispositivos informacionais de todos os tipos. Escrita, leitura, visão, audição, criação e aprendizagem são capturadas por uma informática cada vez mais avançada. A Tecnologia da Informação e Comunicação tem um papel significativo na criação desse ambiente colaborativo e, posteriormente, em uma gestão do conhecimento. No entanto, é importante ressaltar que a tecnologia da informação e comunicação desempenha seu papel apenas promovendo a infraestrutura, pois o trabalho colaborativo e a gestão do conhecimento envolvem também aspectos humanos, culturais e de gestão (Silva, 2003).

2.9 Entretanto, o parque de equipamentos que forma o ambiente de segurança da informação na sede deste Instituto está, em sua maior parte, descontinuada pelos fabricantes e na sua totalidade sem contrato de manutenção e de garantia de funcionamento, o que coloca em risco a continuidade dos serviços de TI disponibilizados pela coordenação geral de tecnologia da informação, bem como os serviços prestados pelo Ibama.

2.10 A falta ou indisponibilidade destes recursos, traria a parada da rede de comunicação interna e externa, trazendo prejuízos à continuidade operacional das áreas e gera atrasos na entrega dos projetos de negócio. A indisponibilidade destes recursos certamente traria prejuízos à execução dos serviços administrativos da instituição, situação que acarretaria transtornos à população que acessa o Instituto através dos recursos de tecnologia da informação e, consequentemente, danos à sua imagem.

2.11 No presente contexto, convém citarmos o princípio da economicidade cuja meta é a obtenção da melhor relação custo-benefício possível que uma alocação de recursos financeiros, econômicos ou patrimoniais possa alcançar, bem como o princípio da eficiência, que exige o aperfeiçoamento dos serviços e atividades, em busca de melhores resultados e do atendimento ao interesse público com ênfase em maiores índices de adequação, eficácia e satisfação.

2.12 A presente necessidade está ainda em consonância com a "EGD - Estratégia de Governança Digital" do Governo Federal, que pretende convergir os esforços de infraestruturas, plataformas, sistemas e serviços dos órgãos que compõem o Sistema de Administração dos Recursos de Tecnologia da Informação – SISP com as iniciativas de governo digital e sensibilizar os dirigentes do Governo Federal sobre a importância da governança digital para o Estado brasileiro. Dentro do EGD podemos destacar os seguintes conceitos que vão ao encontro da presente necessidade deste Instituto, a saber:

2.12.1 **Governança Digital**: utilização, pelo setor público, de tecnologias da informação e comunicação com o objetivo de melhorar a informação e a prestação de serviços, incentivando a participação dos cidadãos no processo de tomada de decisão e tornando o governo mais responsável, transparente e eficaz (Verma et al., National Informatics Centre of India, 2005).

2.12.2 **Segurança da Informação e Comunicação**: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (Brasil, 2008).

2.12.3 **Tecnologia da Informação e Comunicação (TIC)**: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações.

2.12.4 **Tecnologias Digitais**: referem-se às TIC, incluindo a internet, tecnologias e dispositivos móveis, desenvolvimento de serviços e aplicações e análise de dados, utilizados para melhorar a geração, coleta, troca, agregação, combinação, análise, acesso, busca e apresentação de conteúdo digital (OECD, 2014).

2.13 A aquisição dos novos ativos de Appliance de Firewall visa assegurar a continuidade da segurança na comunicação de dados externamente e entre os ativos de tecnologia do núcleo de rede de dados do Ibama. Os equipamentos atuais que desempenham tais funções encontram-se em processo de descontinuação do serviço de suporte pelos fabricantes. A segurança das informações trafegadas na rede de dados do Ibama serão significativamente comprometidas caso não haja a renovação dos Appliances de Firewall, que serão utilizados como core da Área de Segurança.

2.14 Assim posto, a presente demanda, culmina na necessidade de contratação de pessoa jurídica de direto privado especializada no segmento de Segurança da Informação para o fornecimento de solução de Appliances de Firewall (Solução de Segurança), incluindo instalação, capacitação técnica, garantia e suporte.

## 3 DA DESCRIÇÃO DA SOLUÇÃO DE TIC

3.1 A utilização das Tecnologias da Informação e Comunicação pelas pessoas e organizações vem crescendo significativamente, de forma a suportar processos de negócio e organizacionais, comunicação e decisão mais ágeis. Uma arquitetura simples provê maior flexibilidade à TI para entregar novas aplicações e serviços de acordo com a evolução das necessidades e demandas.

3.2 A crescente disseminação de ataques às redes de computadores, em especial às redes do Governo, requer tratamento adequado, visando proteger o ambiente computacional do IBAMA. Este contexto reforça a necessidade de proteção da informação contra acessos sem autorização, alterações indevidas ou indisponibilidade.

3.3 Para responder ao cenário digital atual, explanado mais abaixo, propomos a aquisição de um novo sistema de firewall com recursos de Next Generation Firewall. Dentre as melhorias que poderão ser obtidas, podemos destacar:

3.3.1 Controle granular das aplicações web permitidas e bloqueadas, priorização de tráfego por tipo de aplicação e comutação automática entre links de internet. Isto possibilitará maior preparação para enfrentar os desafios de hoje ligados à segurança da informação.

3.3.2 As soluções de Next Generation Firewall integram diferentes tipos de proteção, tais como antivírus de perímetro, IPS (Sistema de Prevenção de Intrusão), firewall de camada de aplicação, filtro de navegação na Internet, entre outros, em um único equipamento, reduzindo o custo de manutenção e administração. Estas vêm sendo amplamente utilizadas por órgãos que precisam estar conectados de forma segura.

3.4 Nesse modelo, os Appliances de Firewall atuando em Alta disponibilidade ficarão à frente da topologia, recebendo as informações que chegam externamente e segmentando para os ambientes internos, trazendo a segurança não somente no trafego norte-sul, mas também na troca de dados leste-oeste. Com isso se permite uma maior segurança das informações e controle do tráfego interno, com abordagens para todas as aplicações e sistemas utilizados hoje no ambiente em produção, com total controle e filtro de conteúdo acessado pela WEB. Desta forma a gerência se torna completa com a visibilidade que a TIC terá dos acessos internos e externos.

3.5 A solução consiste na aquisição de equipamentos de Firewall (Appliances) que deverão operar em alta disponibilidade. Esta topologia mostra-se, mais escalável, robusta, resiliente e de menor custo em relação a topologia tradicional baseada na utilização de equipamentos individuais.

3.6 Assim posto, a composição da solução pode ser verificada no escopo de fornecimento em **Das Quantidades Demandadas**.

## 4 DAS QUANTIDADES DEMANDADAS

| | LOTE 01 | | |
|---|---|---|---|
| **ITEM** | **DESCRIÇÃO** | **UNIDADE** | **QUANTIDADE** |
| 1 | Solução de segurança (Firewall de Próxima Geração) com Subscrição e Produto, Incluindo instalação e transferência de conhecimento. Com 3 anos de garantia do fabricante. | UN | 02 |

**Tabela de Escopo de Fornecimento**

4.1 Para esta pretendida contratação não será aceito cotação parcial, sendo obrigatório a cotação total conforme as quantidades da Tabela de Escopo de fornecimento. O entendimento prevalecente é no sentido de que a previsão de cotação parcial de item não é obrigatória, sendo possível à Administração exigir dos licitantes a cotação total. (Itens 27 e 28 do Parecer nº. 098/2016/CJU-RN/CGU/AGU)

## 5 DA ESPECIFICAÇÃO TÉCNICA

5.1 As especificações técnicas constam do APÊNDICE A - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 6 DAS COTAS RESERVADAS

6.1 Não será aplicado o disposto no Art. 8º do Decreto nº 8.538 de 06 de outubro de 2015, considerando a inviabilidade técnica e econômica para o parcelamento do objeto da presente contratação, bem como consideradas as suas respectivas peculiaridades, interdependência e natureza acessória entre as parcelas do objeto.

## 7 ENQUADRAMENTO EM SOLUÇÃO DE TI

7.1 A IN STI/MPOG n° 04/2014 considera, em seu inciso X, do art. 2º, que "Solução de Tecnologia da Informação é o conjunto de bens e serviços de Tecnologia da Informação e automação que se integram para o alcance dos resultados pretendidos com a contratação".

7.2 Em virtude da consideração acima, o entendimento acerca da conceituação apresentada na IN n° 04/2014 STI/MPOG se baseia na integração de bens, serviços de TI e automação, tendo como finalidade o alcance dos resultados pretendidos pela contratação, que, no processo em questão, refere-se à solução de softwares e serviços especializados no produto com repasse de conhecimento e serviços técnicos especializados.

7.3 Considerando que uma solução de TI engloba todos os elementos (bens, serviços de TI e automação) necessários que se integram para o alcance dos resultados pretendidos com a contratação, de modo a atender à necessidade que a desencadeou, pode-se afirmar que a contratação em questão compreende uma solução de tecnologia, uma vez que compreende uma solução integrada de hardware, software e serviços especializados em uma única infraestrutura computacional.

7.4 Portanto, a contratação ora pretendida enquadra-se em solução de TI, pois refere-se à contratação de uma solução de tecnologia da informação o qual deverá seguir o estabelecido na IN nº 04/2014 STI/MPOG que 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.

7.5 Não obstante a IN 04/2014 seja específica para órgãos integrantes do SISP, do Poder Executivo Federal, o Decreto nº 7.174/2010, que é norma hierarquicamente superior, foi editado com previsão de abrangência e aplicação em toda a área federal. Sendo o Ibama unidade setorial do SISP, seguirá a aplicabilidade da IN nº 04/2014, e subsidiariamente ao decreto acima mencionado no que for pertinente às contratações de bens e serviços de TI.

## 8 DA CONTRATAÇÃO DE SOLUÇÃO ÚNICA DE TI

8.1 O objeto da pretendida contratação, bem como a composição dos itens do escopo de fornecimento detalhado em DAS QUANTIDADES DEMANDADAS, que formam o conjunto de bens e serviços a serem contratados, configuram uma única solução de Tecnologia da Informação.

8.2 Todos os itens do escopo de fornecimento possuem correlação entre si e são elementos inseparáveis de uma mesma e única solução de Tecnologia da Informação para prover a infraestrutura desejada de ativos de Appliances de Firewall.

8.3 Assim posto, o presente TR está em conformidade com o artigo 5º, inciso I, da IN 04/2014 e alterações, que preceitua que: "*Não poderão ser objeto de contratação mais de uma Solução de Tecnologia da Informação em um único contrato*".

## 9 DO CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

9.1 A presente contração deverá será realizada na modalidade de **PREGÃO ELETRÔNICO**, do tipo **MENOR PREÇO**, em observância ao Art. 4º do Decreto nº 5.450/05, devido ao fato de que os bens e serviços são considerados comuns, conforme as características previstas no Art. 1º da Lei nº 10.520/02.

## 10 DOS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

10.1 A **CONTRATADA** deverá adotar práticas de sustentabilidade ambiental na execução do objeto, quando couber, conforme disposto na Instrução Normativa STI nº 01/2010, de 19 de janeiro de 2010, do Ministério do Planejamento e Gestão.

10.2 O ambiente físico da **CONTRATADA** para fins de execução do serviço deve ser compatível com o disposto na NR17 do Ministério do Trabalho e Emprego – MTE e na recomendação técnica DSST nº 01/2005 do Ministério do Planejamento, Desenvolvimento e Gestão.

## 11 ESPECIFICAÇÃO DOS REQUISITOS DA CONTRATAÇÃO

11.1 Requisitos de Negócio:

11.1.1 Os requisitos de negócio são aqueles que independem de características tecnológicas e que definem as necessidades e os aspectos funcionais da Solução de Tecnologia da Informação.

11.1.2 O Plano Diretor de Tecnologia da Informação e Comunicações do Ibama (PDTIC) 2017-2019 reflete o amadurecimento do nível de governança em Tecnologia da Informação e Comunicações (TIC) do Instituto, fruto da atuação do Comitê de Tecnologia da Informação (CTI) e do empenho e árduo trabalho dos servidores desta Instituição, que com afinco e competência participaram da elaboração desta importante ferramenta para o alcance de sua missão institucional.

11.1.3 Buscando um alinhamento com as demais áreas e buscando alcançar melhores resultados, o Ibama definiu em seu Planejamento vigente sua missão, que é a de: "*Garantir a entrega das ações e serviços de Tecnologia da Informação e Comunicações com qualidade para o alcance dos objetivos estratégicos do Ibama*".

11.1.4 Como perspectiva, destaca-se a visão de futuro da CGTI: "Ser reconhecida pelo Ibama como unidade de excelência no provimento de soluções de Tecnologia da Informação

e Comunicações com maior agilidade e qualidade a fim de contribuir diretamente para o cumprimento da missão institucional".

11.1.5 O planejamento estratégico de TIC é necessário para gerenciar todos os recursos de TIC de forma alinhada com as prioridades e estratégias do Ibama. O PDTIC Ibama 2017-2019 define como os serviços e recursos de Tecnologia da Informação e Comunicações contribuirão para o alcance dos 17 (dezessete) objetivos estratégicos descritos no Plano Estratégico Institucional 2016-2019:

11.1.5.1 OE.PEI.01 – Promover o licenciamento como mecanismo de desenvolvimento sustentável do país;

11.1.5.2 OE.PEI.02 – Ampliar a efetividade do controle ambiental;

11.1.5.3 OE.PEI.03 – Promover e aprimorar a regulação da área ambiental;

11.1.5.4 OE.PEI.04 – Prover dados e informações ambientais;

11.1.5.5 OE.PEI.05 – Desenvolver e fortalecer a comunicação institucional;

11.1.5.6 OE.PEI.06 – Aprimorar e padronizar regras, métodos e processos de trabalho;

11.1.5.7 OE.PEI.07 – Fortalecer instrumentos e processos de governança;

11.1.5.8 OE.PEI.08 – Promover parcerias interinstitucionais de gestão ambiental;

11.1.5.9 OE.PEI.09 – Fortalecer a coordenação e integração institucional;

11.1.5.10 OE.PEI.10 – Aprimorar a gestão da informação e do conhecimento;

11.1.5.11 OE.PEI.11 – Fortalecer o atendimento ao cidadão;

11.1.5.12 OE.PEI.12 – Fortalecer, desenvolver e valorizar o quadro de pessoal;

11.1.5.13 OE.PEI.13 – Aprimorar os mecanismos gestão de pessoas;

11.1.5.14 OE.PEI.14 – Promover a modernização tecnológica do Ibama;

11.1.5.15 OE.PEI.15 – Gerir a infraestrutura e a logística de forma eficiente e efetiva;

11.1.5.16 OE.PEI.16 – Promover a cultura de gestão por resultados;

11.1.5.17 OE.PEI.17 – Buscar sustentabilidade financeira e orçamentária.

11.1.6 A demanda está ainda alinhada aos objetivos estratégicos do EGD do Governo Federal, bem como ao PDTI do Ibama, a saber:

11.2 A demanda está ainda alinhada aos objetivos estratégicos do EGD do Governo Federal, bem como ao PDTI do Ibama, a saber:

1.1.1.1 Alinhamento ao EGD:

1.1.1.1.1 OE.02 - Ampliar o uso de TIC para promover a transparência e dar publicidade à aplicação dos recursos públicos;

1.1.1.1.2 OE.03 - Garantir a segurança da informação e comunicação do Estado e o sigilo das informações do cidadão;

1.1.1.1.3 OE.05 - Melhorar a governança e a gestão por meio do uso da tecnologia;

1.1.1.1.4 OE.07 - Compartilhar e integrar dados, processos, sistemas, serviços e infraestrutura.

1.1.1.2 Alinhamento ao PDTI Ibama 2017-2019:

1.1.1.2.1 A presente contratação visa atender a necessidade:

1.1.1.2.1.1 N-33, Aquisição e implantação de solução de segurança de rede corporativa (firewall, anti-ddos, IPS, IDS, anti-spam, etc.), ação A0501 do PDTIC 2017-2019 do Ibama.

1.1.1.2.2 A necessidade N-33 está associada aos objetivos estratégicos:

OE.1, Fortalecer e consolidar as parcerias técnicas entre as unidades descentralizadas e a área de TIC da Sede;

OE.2 – Garantir a infraestrutura de TIC apropriada às necessidades tecnológicas do Ibama, incluindo a contínua modernização das tecnologias utilizadas;

OE.3, Aprimorar os níveis de satisfação no atendimento dos usuários de TIC do Ibama;

OE.4 – Promover a segurança da informação, garantindo disponibilidade, confidencialidade e integridade dos dados.

11.3 Requisitos de Capacitação:

11.3.1 Os requisitos de capacitação estão especificados no APÊNDICE A deste Termo de Referência.

11.4 Requisitos legais:

11.4.1 Este TR foi elaborado de acordo com o Ordenamento Jurídico Nacional que regulamenta o processo de aquisições para a Administração Pública; Lei n. 8.666 de 21 de junho de 1993, Lei n. 10.520 de 17 de julho de 2002 e o Decreto n. 5.450, de 31 de maio de 2005, e constitui peça integrante, indispensável e inseparável do processo licitatório, visando viabilizar a aquisição dos bens e serviços descritos neste TR e seus anexos;

11.4.2 As Instruções Normativas STI/MP nº 01 de 2010 e nº 04 de 2014, e alterações, ambas da Secretaria de Tecnologia da Informação do Ministério do Planejamento, Desenvolvimento e Gestão que regulamentam os itens mínimos necessários para a composição do Termo de Referência, e também a Instrução Normativa STI/MP nº 05 de 27 de junho de 2014 e nº 7 de 29 de agosto de 2014, que dispõe sobre os

procedimentos administrativos básicos para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral;

11.4.3 Os bens e serviços que constituem o objeto deste TR enquadram-se no conceito de comuns, nos termos da Lei 10.520/02, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado;

11.4.4 Assim, entende-se, S.M.J. 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.

11.5 Requisitos de manutenção:

11.5.1 Os requisitos de manutenção são os definidos e especificados no APÊNDICE A deste Termo de Referência.

11.6 Requisitos temporais:

11.6.1 Os requisitos temporais são:

11.6.1.1 Vide Item DO PAGAMENTO;

11.6.1.2 Vide Item CRONOGRAMA FÍSICO-FINANCEIRO;

11.7 Requisitos de segurança:

11.7.1 Os exigidos pela Política de Segurança da Informação, Informática e Comunicações do Ibama – POSIC, Publicada no DOU de 06/06/2012 (nº 109, Seção 1, pág. 151).

11.7.2 A CONTRATADA deverá garantir a segurança das informações do Ibama e se compromete a não divulgar ou fornecer a terceiros quaisquer dados e informações que tenha recebido deste instituto no curso da prestação dos serviços, a menos que autorizado formalmente e por escrito para tal.

11.7.3 Deverá ser celebrado TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES entre a CONTRATADA e a CONTRATANTE para garantir a segurança das informações.

11.7.4 A CONTRATADA, após a assinatura do contrato, por meio de seu representante, assinará TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO (APÊNDICE "J") em que se responsabilizará pela manutenção de sigilo e confidencialidade das informações a que possa ter acesso em decorrência da contratação.

11.7.5 Além do termo citado, a CONTRATADA deverá apresentar para cada funcionário que vier a executar atividades referentes ao objeto da contratação, TERMO DE CIÊNCIA (APÊNDICE "K") em que seus profissionais declaram estar cientes das responsabilidades pela manutenção de sigilo e confidencialidade.

11.8 Requisitos sociais, ambientais e culturais:

11.8.1 A CONTRATADA deverá atender no que couber, os critérios de sustentabilidade ambiental. Destaca-se, as recomendações contidas no Capítulo III, DOS BENS E SERVIÇOS, com ênfase no art. 5º da Instrução Normativa nº 01/2010 STI/MPOG, bem como, o Decreto nº 7.746/2012 que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável e a Lei nº 12.305/2010 que institui a política de resíduos sólidos, no que couber.

11.8.2 É dever da CONTRATADA observar entre outras: o menor impacto sobre recursos naturais como flora, fauna, ar, solo e água; preferência para materiais, tecnologias e matérias-primas de origem local; maior eficiência na utilização de recursos naturais como água e energia; maior geração de empregos, preferencialmente com mão de obra local; maior vida útil e menor custo de manutenção do bem e da obra; uso de inovações que reduzam a pressão sobre recursos naturais; e origem ambientalmente regular dos recursos naturais utilizados nos bens, serviços e obras.

11.9 Requisito de arquitetura tecnológica:

11.9.1 A arquitetura tecnológica, especificações e peculiaridades da solução consta assentada no APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

11.10 Requisitos de projeto e de implementação:

11.10.1 A arquitetura tecnológica, especificações e peculiaridades da solução constam assentadas no APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

11.11 Requisitos de implantação:

11.11.1 Conforme estabelecido no, APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS.

11.12 Requisitos de garantia e manutenção:

11.12.1 A CONTRATADA deverá oferecer garantia para os itens ofertados, por um período de 36 (trinta e seis) meses, incluindo suporte no formado 8x5xNBD (oito horas, cinco dias por semana) com troca de equipamentos e peças que demonstrem mal funcionamento em até 24 horas úteis.

11.13 Requisitos de capacitação:

11.13.1 Os requisitos de capacitação estão especificados no APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

11.14 Requisitos de experiência profissional da equipe:

11.14.1 Conforme estabelecido no APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

11.15 Requisitos de formação da equipe:

11.15.1 Conforme estabelecido no APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

11.16 Requisitos de metodologia de trabalho:

11.16.1 Conforme estabelecido no APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

11.17 Requisitos de segurança da informação:

11.17.1 Conforme estabelecido no APÊNDICE "A" - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 12 DA PROVA DE CONCEITO

12.1 Havendo necessidade de esclarecimentos, **exclusivamente a critério do Ibama**, o Pregoeiro, sustentada por solicitação da equipe técnica, poderá solicitar à licitante, cuja proposta tenha

sido aceita quanto à compatibilidade de preço, amostra dos produtos ofertados, que deverá ser encaminhada a Coordenação Geral de Tecnologia da Informação, situado no Ibama, SCEN Trecho 2 - Edifício Sede - CEP 70.818-900 - Brasília-DF - Fone: (61) 3316-1212, no horário das 09h às 12h e de 14h às 18h, no prazo de 05 (cinco) dias úteis, a partir da solicitação.

12.2 O prazo para a avaliação das amostras será de até 05 (cinco) dias a partir do momento do recebimento destas, sendo possíveis prorrogações neste prazo por despacho fundamentado do Pregoeiro.

12.3 O Ibama resguarda-se ao direito de solicitar apoio técnico da licitante para a realização da verificação. Nesta hipótese, o técnico designado pela licitante deverá executar a verificação na amostra conforme orientações do integrante da equipe de avaliação.

12.4 A previsão de envio de amostras pode ser solicitado, a critério do Ibama, exclusivamente a licitante vencedora, visando identificar se os produtos descritos na proposta comercial da empresa atendem a todos os requisitos do Termo de Referência e aos padrões de desempenho solicitados.

12.5 O Ibama se reserva o direito de não realizar a solicitação das amostras caso entenda que a documentação ofertada junto com a proposta e as pesquisas realizadas pelo corpo técnico do Ibama são suficientes para a aceitação da proposta;

12.6 O procedimento de avaliação das amostras, quando solicitado, será executado conforme descrito no APÊNDICE C – PROCEDIMENTOS DE AVALIAÇÃO DAS AMOSTRAS.

12.7 A homologação das amostras é um ato exclusivo do Ibama, não cabendo as licitantes requisitar a realização da amostra como forma de comprovação que a proposta beneficiária atende aos requisitos do edital.

## 13 DA NATUREZA DA CONTRATAÇÃO

13.1 Os bens e serviços que constituem o objeto deste TR enquadram-se no conceito de **comuns,** nos termos da Lei 10.520/02, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado.

## 14 DAS OBRIGAÇÕES DAS PARTES

14.1 OBRIGAÇÕES DA CONTRATANTE

14.1.1 Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;

14.1.2 Encaminhar formalmente a CONTRATADA a demanda, por meio de **OF - Ordem de Fornecimento**, de bens e/o serviços, de acordo com os critérios estabelecidos no Termo de Referência ou Projeto Básico, observando-se o disposto no arts. 19 e 33 da IN04 de 11/09/2014;

14.1.3 Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e

encaminhando os apontamentos à autoridade competente para as providências cabíveis;

14.1.4 Notificar a CONTRATADA por escrito da ocorrência de eventuais imperfeições no curso da execução dos serviços, fixando prazo para a sua correção;

14.1.5 Não permitir que os empregados da CONTRATADA realizem horas extras, exceto em caso de comprovada necessidade de serviço, formalmente justificada pela autoridade do órgão para o qual o trabalho seja prestado e desde que observado o limite da legislação trabalhista;

14.1.6 Pagar à CONTRATADA o valor resultante dos produtos e da prestação do serviço, no prazo e condições estabelecidas no Edital e seus anexos;

14.1.7 Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura fornecida pela contratada, em conformidade com o art. 36, §8º da IN STI/MPOG N. 02/2008.

14.1.8 Submeter, previamente, a PFE, para análise jurídica, todo e qualquer aditivo contratual;

14.2 OBRIGAÇÕES DA CONTRATADA

14.2.1 Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta;

14.2.2 Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

14.2.3 Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com os artigos 14 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990), ficando a Contratante autorizada a descontar da garantia, caso exigida no edital, ou dos pagamentos devidos à Contratada, o valor correspondente aos danos sofridos;

14.2.4 Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor;

14.2.5 Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso;

14.2.6 Apresentar à Contratante, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço;

14.2.7 Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas na legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE;

14.2.8 Atender as solicitações da CONTRATANTE quanto à substituição dos empregados alocados, no prazo fixado pelo fiscal do contrato, nos casos em que ficar constatado descumprimento das obrigações relativas à execução do serviço, conforme descrito neste Termo de Referência;

14.2.9 Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração;

14.2.10 Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função;

14.2.11 Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços;

14.2.12 Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;

14.2.13 Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

14.2.14 Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

14.2.15 Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

14.2.16 Indicar formalmente preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

14.2.17 Atender prontamente quaisquer orientações e exigências do fiscal do contrato, inerentes à execução do objeto contratual;

14.2.18 Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela CONTRATANTE;

14.2.19 Propiciar todos os meios e facilidades necessárias à fiscalização da Solução de Tecnologia da Informação pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcialmente, em qualquer tempo, sempre que considerar a medida necessária;

14.2.20 Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

14.2.21 Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da Solução de Tecnologia da Informação;

14.2.22 Manter a produtividade ou a capacidade mínima de fornecimento da Solução de Tecnologia da Informação durante a execução do contrato, conforme art. 18, inciso I, alínea “g”;

14.2.23 Fornecer, sempre que solicitado, amostra para realização de Prova de Conceito para fins de comprovação de atendimento das especificações técnicas; e

14.2.24 Ceder, quando for o caso, os direitos de propriedade intelectual e direitos autorais da Solução de Tecnologia da Informação sobre os diversos artefatos e produtos produzidos ao longo do contrato, incluindo a documentação, os modelos de dados e as bases de dados, à Administração.

14.2.24.1 Vide em DIREITOS DE PROPRIEDADE INTELECTUAL E DIREITOS AUTORAIS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO quando serão aplicados os direitos de propriedade intelectual.

14.2.25 Cumprir fielmente os requisitos constantes em DOS CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL.

## 15 DA SUBCONTRATAÇÃO DO OBJETO

15.1 Dispõe a Lei nº 8.666/93, em seu art. 72, que a CONTRATADA, na execução do contrato, sem prejuízo das responsabilidades contratuais e legais, poderá subcontratar partes do serviço ou fornecimento, até o limite admitido, em cada caso, pela Administração. A subcontratação, desde que prevista no instrumento convocatório, possibilita que terceiro, que não participou do certame licitatório, realize parte do objeto.

15.2 Entretanto, à Administração CONTRATANTE cabe, exercitando a previsão do edital, autorizar ou proibir a subcontratação. Por isto, para a pretendida contratação será admitida a subcontratação do objeto licitatório apenas nas condições a seguir:

15.2.1 Não se admitirá a subcontratação para o fornecimento de bens;

15.2.2 Para os serviços de instalação e manutenção poderá ocorrer a subcontratação do Fabricante ou de empresa credenciada ao Fabricante;

15.2.3 Para garantia ou manutenção que a critério da CONTRATADA seja necessário ser prestado pelo FABRICANTE da solução, poderá ocorrer a subcontratação, pois entende-se que o FABRICANTE é parte fundamental à garantia de funcionamento da solução, onde neste caso, poderá a CONTRATADA utilizar de todo e qualquer serviço do FABRICANTE ao fiel cumprimento das obrigações contratuais, desde que não acarrete ônus a CONTRATANTE;

15.2.4 Mesmo nas duas hipóteses anteriores, permanece a responsabilidade integral da CONTRATADA pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante a CONTRATANTE pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto .

## 16 DO ACORDO DE NÍVEL DE SERVIÇO.

16.1 A execução contratual será acompanhada e fiscalizada por representantes da CONTRATANTE, que poderá utilizar-se da contratação de terceiros para assisti-la e subsidiá-la de informações pertinentes a essa atribuição, em consonância com as disposições do art. 67 da Lei nº 8.666/1993.

16.2 A fiscalização não exclui nem reduz a responsabilidade das empresas contratadas pelos danos causados à contratante ou a terceiros decorrentes de ato ilícito na execução do contrato. Além disso, a ocorrência de irregularidades não implica em corresponsabilidade da contratante.

16.3 A avaliação da qualidade e da adequação dos serviços ocorrerá a cada entrega de produtos previstos nas OFs, e será realizada pelo Fiscal Técnico do Contrato com base nos indicadores definidos neste documento, a partir dos registros das demandas mantidos pela CONTRATANTE. Para avaliar a qualidade dos serviços prestados, o Instituto poderá utilizar os registros gerados por outras empresas contratadas.

16.4 O fornecimento de bens e a execução de serviços deverão atender ao ACORDO DE NÍVEL DE SERVIÇO estabelecido pelo indicador abaixo. A CONTRATADA estará sujeita, garantido o contraditório e a ampla defesa, às sanções administrativas em função dos indicadores obtidos abaixo da faixa de ajuste. A aplicação dos ajustes do pagamento não exclui a aplicação de multas e sanções previstas neste documento.

16.5 Indicador de Atraso nas Execuções (IAE)

| | |
|---|---|
| **Finalidade:** | Garantir o atendimento à execução das OFs dentro do prazo acordado. |
| **Escopo de Aplicação:** | Este indicador se aplica ao itens do escopo de fornecimento. |
| **Forma de Aferição:** | É apurado o indicador de atraso entre a data acordada para entrega/execução da OF - Ordem de Fornecimento, e a data efetiva data de recebimento pela CONTRATANTE. A aferição será realizada pelo Fiscal Técnico do Contrato. |
| **Mecanismo de Cálculo:** | $$IAE = \frac{QDA}{PPE}$$ Onde:<br>• *Quantidade de Dias de Atraso – QDA* é a quantidade de dias decorridos após o prazo de entrega. Ela é obtida pela subtração da quantidade de dias efetivamente utilizados para a entrega subtraídos da quantidade de dias planejados para a entrega.<br>• *Prazo Planejado para Entrega – PPE* é a quantidade de dias planejados para a entrega, conforme estabelecido neste Termo de Referência.<br>• Ambos são medidos em dias úteis. Serão considerados dias corridos apenas quando a característica do serviço exigir, a exemplo dos serviços emergenciais (esse fato deverá ficar explícito na OF) e estejam previstos neste Termo de Referência. Caso contrário, serão considerados apenas os dias úteis. |

| | |
|---|---|
| | • Indicador de Atraso nas Execuções (IAE) e indicador de atraso na execução da OF - Ordem de Fornecimento. |
| **Periodicidade:** | A cada OF emitida. |
| **Cobertura:** | Durante toda a vigência contratual. |
| **Faixas de Ajuste no Pagamento:** | Se:<br>• $IAE \leq 0$, não há ajuste, uma vez que o nível desejado foi atingido;<br>• $0 < IAE \leq 0{,}3$, a empresa contratada será comunicada do fato, uma vez que foi constatado um atraso, entretanto sem aplicação de glosa ou penalidade;<br>• $IAE > 0{,}3$, será solicitada uma justificativa à empresa contratada e, caso o Ibama não acate a justificativa, será aplicado um fator de desconto conforme a expressão abaixo:<br>$$VF = VI \times \left(1 - \frac{IAE}{10}\right)$$<br>Onde:<br>• *Valor Final – VF* é o valor final da demanda, projeto ou etapa, após a aplicação do desconto referente a este indicador. Esse valor descontado será o faturado pela empresa contratada;<br>• *Valor Inicial – VI* é o valor aferido da demanda, projeto ou etapa antes da aplicação do desconto referente a este indicador. |
| **Sanções:** | $IAE > 2{,}0$ será solicitada uma justificativa à empresa contratada e, caso o Ibama não acate a justificativa, estará poderá caracterizar a inexecução da demanda, projeto ou etapa, com a aplicação das penalidades previstas no contrato. |

16.6 Deverão ser consideradas ainda as especificações contidas no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 17 DA ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO

17.1 Todo e qualquer fornecimento se dará mediante demanda da CONTRATANTE, situação em que será emitida a OF - Ordem de Fornecimento, conforme APÊNDICE G – MODELO DE ORDEM DE FORNECIMENTO.

17.2 Os serviços serão executados nos locais e endereços descritos nas OFs, respeitada o APÊNDICE M - RELAÇÃO ENDEREÇOS DAS LOCALIDADES.

17.3 O prazo de entrega e/ou execução da OF consta no cronograma físico financeiro detalhado e apresentado no item Do Pagamento.

17.4 Os bens e/ou serviços que compõem a solução serão recebidos:

17.4.1 **Provisoriamente**, a partir da entrega e/ou execução, para efeito de verificação da conformidade com as especificações constantes do Edital e da proposta, que se dará até 15 (quinze) dias da data de entrega.

17.4.1.1 Ao término deste recebimento será emitido o Termo de Recebimento Provisório da OF - Ordem de Fornecimento, vide APÊNDICE H – TERMO DE RECEBIMENTO PROVISÓRIO.

17.4.2 **Definitivamente**, no prazo de 15 (quinze) dias após a emissão dos Termo de Recebimento Provisório.

17.4.2.1 Ao término deste recebimento será emitido o Termo de Recebimento Definitivo – TRD da OF - Ordem de Fornecimento, vide APÊNDICE I - TERMO DE RECEBIMENTO DEFINITIVO.

17.4.3 A Administração rejeitará, no todo ou em parte, a entrega dos serviços em desacordo com as especificações técnicas exigidas.

17.5 Da Aceitação

17.5.1 A recusa parcial ou total no atendimento de uma OF - Ordem de Fornecimento emitida, será oficiada à CONTRATADA pela CONTRATANTE, que deverá prontamente prestar o serviço de acordo com o estabelecido na respectiva OF;

17.5.2 A aceitação definitiva dar-se-á após a assinatura do termo de recebimento definitivo, correspondente a cada OF.

## 18 DO MODELO DE EXECUÇÃO DO CONTRATO

18.1 CONTRATADA deverá elaborar um plano de comunicação em conjunto com a CONTRATANTE de acordo com as seguintes diretrizes:

18.1.1 Disponibilizar um profissional responsável pelo relacionamento com a CONTRATANTE, definindo as formas de integração das equipes.

18.1.2 Prever reuniões, com periodicidade a ser definida pelas partes, para avaliação dos resultados e propor recomendações para a execução dos serviços.

18.1.3 Descrever o processo e os procedimentos para a troca de informações que utilize mecanismos formais de comunicação; tais como: e-mail, ata de reunião ou sistema de informação que contemple formas de registro e acompanhamento dos assuntos tratados nas reuniões periódicas.

## 19 DO MODELO DE GESTÃO DO CONTRATO

19.1 O Ibama será responsável pela gestão do contrato e pelo atesto quanto à aderência aos padrões de qualidade exigidos dos produtos e serviços entregues.

19.2 A CONTRATADA será responsável pela execução dos serviços e gestão dos recursos humanos, físicos e tecnológicos inerentes ao escopo da contratação.

19.3 Todos os produtos a serem entregues pela CONTRATADA serão solicitados mediante OF - Ordem de Fornecimento.

19.4 Todos os serviços a serem prestados pela CONTRATADA serão executados mediante OF - Ordem de Fornecimento.

19.5 Os níveis mínimos de serviço exigidos – NMSE (nível de serviço requerido) serão aferidos e avaliados regularmente pelo Gestor e Fiscais do Contrato, conforme definido no item **ACORDO DE NÍVEL DE SERVIÇO** deste documento.

## 20 DA OF - ORDEM DE FORNECIMENTO

20.1 Será utilizado o procedimento de abertura de OF - Ordem de Fornecimento para as comunicações formais através de canal definido entre as partes.

20.2 A CONTRATADA poderá ofertar um modelo de ordem de serviço para aprovação pela comissão de recebimento, onde constem, no mínimo, os campos descritos abaixo, observando os prazos previstos no item Níveis Mínimos de Serviço Exigido:

20.3 Nº da ordem de serviço;

20.4 Nº do contrato administrativo;

20.5 Data da prestação dos serviços;

20.6 Descrição dos serviços a serem executados;

20.7 Unidade de medida;

20.8 Indicadores contratuais exigidos;

20.9 Prazo e local de execução dos serviços;

20.10 Disponibilidade dos serviços;

20.11 Valor Total e Unitário.

20.12 Deve ser assinada e carimbada pelo Gestor e Preposto do contrato.

## 21 PAPÉIS E RESPONSABILIDADES

21.1 PELO IBAMA:

21.1.1 Gestor do Contrato:

21.1.1.1 Servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente.

21.1.2 Fiscal Requisitante:

21.1.2.1 Servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação.

21.1.3 Fiscal Técnico:

21.1.3.1 Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato.

21.1.4 Fiscal Administrativo:

21.1.4.1 Servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos.

21.2 PELA CONTRATADA

21.2.1 Preposto:

21.2.1.1 Representante da CONTRATADA, responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Ibama, incumbido de receber, diligenciar, encaminhar e responder às principais questões técnicas, legais e administrativas referentes ao andamento contratual:

21.2.1.1.1 Fazer a gestão geral do contrato, mantendo o controle de todas as OFs, com o objetivo de garantir a execução dos serviços dentro dos prazos estabelecidos, atendendo a todos os requisitos de qualidade;

21.2.1.1.2 Distribuição das tarefas entre os membros da equipe da **CONTRATADA**;

21.2.1.1.3 Responder, perante o **Ibama**, pela execução técnica das OFs;

21.2.1.1.4 Participar, sempre que solicitado, de reuniões de acompanhamento das atividades referentes às OFs em execução e com representantes do **Ibama**;

21.2.1.1.5 Levar para as reuniões periódicas de acompanhamento as situações não resolvidas em nível de gerência das OFs;

21.2.1.1.6 Realizar a gestão, por parte da **CONTRATADA**, quanto aos aspectos de caráter administrativo e legal do contrato;

21.2.1.1.7 Atender prontamente e dentro do prazo estipulado quaisquer exigências do Gestor inerentes ao objeto do Contrato, sem que disso decorra qualquer ônus extra para o **Ibama**;

21.2.1.1.8 Acompanhar a execução das OFs em andamento e fornecer informações atualizadas ao Gestor do Contrato, sempre que solicitado;

21.2.1.1.9 Assegurar-se de que as determinações da **CONTRATADA** sejam disseminadas junto aos recursos alocados à execução das OFs;

21.2.1.1.10 Informar ao **Ibama** sobre problemas de qualquer natureza que possam impedir o andamento normal dos serviços;

21.2.1.1.11 Elaborar e entregar ao Gestor os documentos referentes ao acompanhamento da execução das OFs;

21.2.1.1.12 Garantir a execução dos procedimentos administrativos referentes aos recursos envolvidos na execução dos serviços contratados;

21.2.1.1.13 Estar apto a prestar tempestivamente todas as informações (por meio de documentos impressos ou digitais) sobre as regularidades fiscais e financeiras da empresa, bem como a manutenção de todos os requisitos contratuais. Irregularidades administrativas ou contratuais poderão ensejar rescisão contratual;

21.2.1.1.14 Supervisionar todos os processos do trabalho, garantindo a qualidade dos serviços prestados e o cumprimento dos Níveis Mínimos de Serviço estabelecidos;

21.2.1.1.15 Propor novas rotinas, processos e fluxos de trabalho, visando maior eficácia no serviço prestado;

21.2.1.1.16 Gerenciar o cumprimento de prazos e prioridades estabelecidos;

21.2.1.1.17 Gerenciar e acompanhar o desempenho da prestação de serviço.

## 22 DA TRANSIÇÃO CONTRATUAL

22.1 Em casos de interrupção contratual e ocorrendo mudança de fornecedor da solução, todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida e/ou utilizada para a execução dos projetos e serviços contratados deverão ser disponibilizados à contratante ou empresa por ela designada em até 30 (trinta) dias corridos após o encerramento do contrato.

22.2 A empresa contratada deverá elaborar o Plano de Transição, no prazo de 60 (sessenta) dias corridos antes do encerramento do contrato, para a transferência integral e irrestrita dos conhecimentos e das competências necessárias e suficientes para promover a continuidade dos serviços. A contratante poderá estabelecer prazo inferior caso haja rescisão contratual.

22.3 Nenhum pagamento será devido à empresa contratada pela elaboração ou pela execução do Plano de Transição. O fato da empresa contratada ou seus representantes não cooperarem ou reterem qualquer informação ou dado solicitado pela contratante, que venha a prejudicar, de alguma forma, o andamento da transição das tarefas e serviços para um novo prestador, constituirá quebra de contrato, sujeitando-a as obrigações em relação a todos os danos causados à contratante.

## 23 TESTES E INSPEÇÕES

23.1 Os serviços serão recebidos após a verificação do atendimento dos Níveis Mínimos de Serviços Exigidos.

23.2 Todas as atividades devem ser relacionadas e fornecidas à **FISCALIZAÇÃO** do **Ibama**.

## 24 INSPEÇÕES E DILIGÊNCIAS

24.1 O **Ibama** poderá, se julgar necessário, realizar inspeções e diligências no ambiente da **CONTRATADA** a fim de garantir que a mesma esteja em condições de fornecer os serviços pretendidos de acordo com a qualidade exigida pelo **Ibama** e em conformidade com o disposto na NR17 do Ministério do Trabalho e Emprego – MTE e na recomendação técnica DSST nº 01/2005 do mesmo órgão.

## 25 DA VISTORIA

25.1 É necessário a realização de "**vistoria**" às áreas envolvidas na prestação dos serviços, para o conhecimento e uniformização de entendimento quanto às condições para a prestação dos serviços ou a emissão de "**Termo de Recusa de Vistoria**". Uma das seguintes opções deve ser escolhida e atendida pela licitante:

25.2 Da Realização da Vistoria:

25.2.1 A vistoria poderá ser realizada por um representante da licitante, acompanhada por um profissional designado pelo IBAMA, impreterivelmente até 2 (dois) dias úteis anterior à data prevista para a realização da abertura da licitação, em data previamente marcada pelo telefone **(61) 3316-1076** em dias úteis, no horário de 9h às 17h.

25.2.2 Ao término da vistoria será emitido, em 2 (duas) vias, o termo de Declaração de Vistoria, conforme modelo constante do Apêndice "D".

25.2.3 A declaração de vistoria deverá ser assinada pelos representantes do Ibama e da Licitante, comprovando que a empresa realizou a vistoria técnica para conhecimento dos serviços necessários, do ambiente tecnológico do Ibama e das condições técnicas para sua realização.

25.2.4 A não apresentação da declaração em sua proposta comercial pode ensejar em desclassificação da proposta.

25.3 Da Recusa de Realização de Vistoria:

25.3.1 A Licitante que optar pela não realização da vistoria deverá apresentar, junto com sua proposta de preços, caso seja a vencedora da etapa de lances, a DECLARAÇÃO DE RECUSA DE VISTORIA, conforme modelo constante do APÊNDICE "E", devidamente assinada pelos seus Representantes Legais.

25.3.2 A Licitante que optar pela não realização da vistoria estará se responsabilizando por todas as condições de fornecimento, não podendo em qualquer momento da execução contratual alegar desconhecimento ou impossibilidade para a prestação dos serviços.

25.3.3 A não apresentação da declaração em sua proposta comercial pode ensejar em desclassificação da proposta.

## 26 CUSTO ESTIMADO DA CONTRATAÇÃO

26.1 A planilha indicativa para previsão orçamentária foi elaborada com base em cotações de mercado, consideradas as especificações produzidas e seguindo as orientações da IN STI/MP 05/2014 e 07/2014.

26.2 O detalhamento dos valores unitários e totais máximos que a administração se dispõe a pagar constam do **APÊNDICE "S" MEMORIAL DE CÁLCULO**.

## 27 ADEQUAÇÃO ORÇAMENTÁRIA

27.1 Conforme DECRETO Nº 7.892, DE 23 DE JANEIRO DE 2013, que Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993., no seu Art. 7º , § 2º, 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.

## 28 ESTIMATIVA DE IMPACTO ECONÔMICO FINANCEIRO

28.1 As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, e correrá por conta dos recursos orçamentários constantes do Orçamento Geral da União, aprovado pela LOA - Lei Orçamentária Anual para o exercício de 2017.

## 29 REGIME DE EXECUÇÃO DO CONTRATO

29.1 Os bens e serviços contratados serão executados na forma de EXECUÇÃO INDIRETA POR PREÇO UNITÁRIO, de acordo com o disposto na Lei nº 8.666/93, art. 6º, VIII, "b".

29.2 O regime de empreitada por preço unitário justifica-se pela necessidade da Administração em contratar os referidos bens e serviços sob demanda, considerando o preço certo das unidades determinadas no escopo.

29.3 Os produtos e serviços serão demandados de acordo com a necessidade do Ibama.

## 30 CRITÉRIOS E REQUISITOS DE HABILITAÇÃO

30.1 Qualificação Técnica:

30.1.1 Apresentar atestado(s) de capacidade técnica para comprovação de execução anterior de atividade pertinente, fornecido por pessoa jurídica de direito público/privado, que comprove ter a LICITANTE prestado serviço de instalação e configuração / migração de Solução de Segurança (Firewall de próxima Geração)

30.1.1.1 No caso de atestados emitidos por empresas privadas, não serão válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da empresa LICITANTE. São consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa LICITANTE, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócia ou possua vínculo com a empresa emitente ou empresa licitante.

30.1.1.2 Em nenhuma circunstância será aceito atestado emitido pela própria licitante;

30.1.2 Caso a LICITANTE não seja a fabricante dos equipamentos da solução de Segurança, deverá apresentar documento, em papel timbrado, emitido pelo fabricante, específico para este órgão e processo, informando que a mesma está apta a comercializar os produtos e serviços ofertados.

30.1.3 A CONTRATADA deverá comprovar em até 15 dias da assinatura do contrato, que firmou junto ao fabricante da solução, contrato de suporte técnico de Firewall. O mesmo deverá estar vinculado a CONTRATANTE e deverá possuir a mesma vigência de Garantia e Suporte Técnico prevista neste Edital.

## 31 ALTERAÇÃO SUBJETIVA

31.1 É admissível a fusão, cisão ou incorporação da **CONTRATADA** com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

## 32 ACOMPANHAMENTO E FISCALIZAÇÃO DO CONTRATO

32.1 O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos arts. 67 e 73 da Lei nº 8.666, de 1993, e do art. 6º do Decreto nº 2.271, de 1997.

32.2 O representante da CONTRATANTE deverá ter a experiência necessária para o acompanhamento e controle da execução dos serviços e do contrato.

32.3 A verificação da adequação do fornecimento deverá ser realizada com base nos critérios previstos neste Termo de Referência.

32.4 A execução dos contratos deverá ser acompanhada e fiscalizada por meio de instrumentos de controle, que compreendam a mensuração dos aspectos mencionados no art. 34 da Instrução Normativa STI/MPOG nº 02, de 2008, quando for o caso.

32.5 O fiscal ou gestor do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos no § 1º do artigo 65 da Lei nº 8.666, de 1993.

32.6 A conformidade do material a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da CONTRATADA que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência e na proposta, informando

as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

32.7 O representante da CONTRATANTE deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 67 da Lei nº 8.666, de 1993.

32.8 O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 77 e 80 da Lei nº 8.666, de 1993.

32.9 As disposições previstas nesta cláusula não excluem o disposto no Anexo IV (Guia de Fiscalização dos Contratos de Terceirização) da Instrução Normativa STI/MPOG nº 02, de 2008, aplicável no que for pertinente à contratação.

32.10 A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

32.10.1 Observar o fiel adimplemento das disposições contratuais;

32.10.2 Solicitar a imediata substituição de funcionário da CONTRATADA que embaraçar ou dificultar o seu atendimento e a sua fiscalização, a seu exclusivo critério;

32.10.3 Rejeitar, no todo ou em parte, os produtos fornecidos em desacordo com as especificações deste Termo de Referência;

32.10.4 Suspender a execução do fornecimento ou dos serviços contratados, sem prejuízo das penalidades a que se sujeita a CONTRATADA, garantido o contraditório e a ampla defesa.

32.11 A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

## 33 SANÇÕES ADMINISTRATIVAS

33.1 Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a CONTRATADA que:

33.1.1 inexecução total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

33.1.2 ensejar o retardamento da execução do objeto;

33.1.3 fraudar na execução do contrato;

33.1.4 comportar-se de modo inidôneo;

33.1.5 cometer fraude fiscal;

33.1.6 não mantiver a proposta.

33.2 A CONTRATADA que cometer qualquer das infrações discriminadas nos subitens acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

33.2.1 Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a CONTRATANTE;

33.2.2 Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

33.2.3 Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

33.2.4 Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a CONTRATADA ressarcir a CONTRATANTE pelos prejuízos causados;

33.2.5 Multa moratória de 2% (dois por cento) sobre o valor do Contrato, pela recusa da licitante adjudicatária em assinar o Contrato, e não apresentar a documentação exigida no Edital para sua celebração, nos prazos e condições estabelecidas, caracterizando o descumprimento total da obrigação assumida, com base no art. 81 da Lei no 8.666, de 1993, independentemente das demais sanções cabíveis;

33.2.6 Multa compensatória 5% (cinco por cento) sobre o valor do contrato, pela inexecução parcial, total ou execução insatisfatória do contrato e pela interrupção da execução do contrato sem prévia autorização da CONTRATANTE, aplicada em dobro na sua reincidência, independentemente das demais sanções cabíveis;

33.2.7 Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

33.3 A incidência das glosas advindas dos níveis mínimos de serviço exigidos poderão ser aplicadas juntamente com as sanções e penalidades, facultada a defesa prévia do interessado no respectivo processo, no prazo de cinco (05) dias úteis;

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

33.5 A LICITANTE que, convocada dentro do prazo de validade de sua proposta, não assinar o Contrato, deixar de entregar documentação exigida no Edital, apresentar documentação falsa, ensejar o retardamento da execução do Contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará impedida de licitar e contratar com a União, e será descredenciada no SICAF, pelo prazo de até dois (02) anos, sem prejuízo das multas previstas em Edital, no Contrato e nas demais cominações legais.

33.6 A CONTRATADA ficará sujeita, com fundamento nos artigos 86 e 87 da Lei n.º 8.666/93, a penalidades, nos casos de inexecução total ou parcial do objeto.

33.7 Em caso de inexecução do contrato, erro de execução, execução parcial (imperfeita), mora de execução e inadimplemento contratual, a CONTRATADA ficará sujeita, ainda, às seguintes penalidades:

33.7.1 A declaração de impedimento para licitar com a Administração Pública dar-se-à pela autoridade máxima do órgão CONTRATANTE nos termos da Lei 8.666 de 1993.

33.8 A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à CONTRATADA, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

33.9 A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à CONTRATANTE, observado o princípio da proporcionalidade.

33.10 As penalidades serão obrigatoriamente registradas no SICAF e, no caso de impedimento de licitar e contratar com a União, a licitante será descredenciada por igual período, sem prejuízo das multas previstas neste TR e das demais cominações legais;

## 34 TABELA DE GRAU DE SANÇÕES ADMINISTRATIVAS

34.1 Além das sanções previstas anteriormente, a CONTRATADA estará sujeita aos critérios de sanções abaixo, conforme o grau corresponde:

| GRAUS DE SANÇÕES ADMINISTRATIVAS | |
|---|---|
| **GRAU** | **CORRESPONDÊNCIA** |
| 01 | Advertência escrita |
| 02 | Multa de 0,2% sobre o valor do Contrato |
| 03 | Multa de 0,3% sobre o valor do Contrato |
| 04 | Multa de 1% sobre o valor do Contrato |

34.2 As glosas nos pagamentos a que se sujeita a CONTRATADA terão como referência:

| REFERÊNCIA PARA SANÇÃO | |
|---|---|
| **DESCRIÇÃO DA REFERÊNCIA** | **GRAU** |
| Permitir a presença de empregado sem crachá nos locais onde haverá a entrega do objeto | Por ocorrência 01 |
| Suspender ou interromper, salvo motivo de força maior ou caso fortuito, a entrega do objeto | Por ocorrência 03 |
| Manter empregado sem qualificação exigida na execução do objeto | Por ocorrência 02 |
| Não substituir, imediatamente, o profissional que seja considerado inapto na execução do objeto, seja por incapacidade técnica, atitude inconveniente, falta de urbanidade ou que venha a transgredir as Normas disciplinares do órgão | Por ocorrência 02 |
| Acumular 2 (duas) advertências no período de 12 (doze) meses | Por ocorrência 02 |
| Acumular 5 (cinco) advertências no período de 12 (doze) meses | Por ocorrência 03 |
| Não zelar pelas instalações do órgão | Por ocorrência 01 |

| | |
|---|---|
| Não efetuar o pagamento de salários, seguros, encargos fiscais e sociais, bem como quaisquer despesas diretas e/ou indiretas relacionadas à execução do objeto | Por ocorrência 03 |
| Na hipótese de rescisão contratual por inexecução total do objeto | Por ocorrência 04 |
| Na hipótese de descumprimento da garantia do objeto | Por ocorrência 03 |
| Não apresentar documentação exigida da empresa ou dos profissionais | Por documento 01 |
| Deixar de prestar quaisquer informações solicitadas no prazo estipulado | Por ocorrência 01 |
| Deixar de realizar transferência completa dos conhecimentos empregados na execução do objeto | Por ocorrência 02 |
| Deixar de realizar transição plena do objeto, com total transferência de conhecimento | Por ocorrência 02 |

## 35 BENEFÍCIOS DIRETOS E INDIRETOS QUE RESULTARÃO DA CONTRATAÇÃO

35.1 **Disponibilidade de serviços**: Incremento do índice de disponibilidade da infraestrutura de Segurança da Informação e troca de dados aos usuários do Ibama, para suportar a unificação de várias unidades de atendimento e vários usuários em uma mesma localidade e mesma infraestrutura.

35.2 **Confiabilidade dos usuários**: Incremento no índice de confiabilidade dos usuários em relação aos serviços de infraestrutura de rede, uma vez que o projeto aumentará a Segurança, disponibilidade e a performance dos serviços de rede.

35.3 **Produtividade dos usuários**: Incremento da produtividade dos Servidores do Ibama através de uma infraestrutura confiável, sem paradas nos serviços por problemas de segurança.

35.4 **Compatibilidade**: Para estes novos produtos a compatibilidade fica assegurada pelos padrões que foram solicitados nas especificações técnicas dos produtos a serem ofertados.

35.5 **Tecnologia**: A tecnologia dos produtos pretendidos está consolidada no mercado, onde esta tecnologia se baseia em melhores práticas, mundialmente utilizados em várias soluções de infraestrutura de Segurança da Informação e controle de acesso de usuários, garantindo assim, o investimento por maior tempo.

35.6 **Confiabilidade na tecnologi**a: Para uma infraestrutura de Firewall de Próxima Geração dedicada a operações de missão crítica, em atividades que demandam disponibilidade constante, a confiabilidade é fato imperioso na escolha do equipamento, pois qualquer parada pode causar grandes transtornos e até prejuízos não mensuráveis para os serviços e a imagem institucional do órgão;

35.7 **Conhecimento Técnico**: O uso de um sistema de segurança prevê um conhecimento específico da tecnologia e a equipe técnica do Ibama deverá receber, no momento da implementação da solução, uma passagem de conhecimento técnico na tecnologia de Firewall, que proverá capacidade para gerenciar a solução e dar suporte de primeiro nível, realizar configurações na solução e criar regras e políticas de segurança baseando-se nas melhores práticas, ampliando assim o conhecimento técnico da equipe.

## 36 MODELO DE PRESTAÇÃO DE SERVIÇOS

36.1 Após a assinatura do Contrato, de acordo com a necessidade, a CONTRATANTE emitirá a(s) OFs, conforme APÊNDICE G – MODELO DE ORDEM FORNECIMENTO.

36.1.1 A data de emissão da OF deverá sempre expressar a data atual de sua emissão e não as datas de empenho e/ou contrato.

36.1.2 Todas as OFs deverão ser atendidas pela CONTRATADA no prazo máximo especificado no item Do Pagamento;

36.1.3 A OF indicará as quantidades, os prazos, os responsáveis pelo recebimento e os locais de entrega conforme APÊNDICE M – RELAÇÃO ENDEREÇOS DAS LOCALIDADES.

36.1.4 Deve ser assinado por todos os empregados da CONTRATADA e empresas indicadas pela CONTRATADA que venham a participar da prestação dos serviços o termo de sigilo e confidencialidade, conforme APÊNDICE J – TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO.

36.2 A Emissão de qualquer OF deverá atender as seguintes premissas:

36.2.1 Só poderá ser emitido OF - Ordem de Fornecimento para itens previamente contratados;

36.2.2 Não há óbice no fatiamento da quantidade de um mesmo item constante do contrato em várias OFs, desde que o somatório das quantidades de cada item em cada OF não ultrapasse a quantidade total de cada item previamente contratado;

36.2.3 OFs para os itens de fornecimento de novos produtos, respectivamente os itens 01 a 15, devem constar em OFs separadas dos demais itens;

36.2.4 OFs para os itens de fornecimento de serviços, respectivamente os itens 16 a 18, devem constar em OFs separadas dos demais itens, bem como separadas entre si;

## 37 DETALHAMENTO DO OBJETO

37.1 Conforme estabelecido no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 38 FORNECIMENTO DOS SOFTWARES

38.1 Conforme estabelecido no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 39 SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO

39.1 Conforme estabelecido no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 40 SERVIÇOS DE IMPLANTAÇÃO

40.1 Conforme estabelecido no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 41 SERVIÇOS DE MANUTENÇÃO, ATUALIZAÇÃO DE VERSÃO E SUPORTE TÉCNICO

41.1 Conforme estabelecido no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 42 CAPACITAÇÃO TÉCNICA

42.1 Conforme estabelecido no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 43 GARANTIA DOS PRODUTOS/SERVIÇOS

43.1 Conforme estabelecido no APÊNDICE “A” - ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS.

## 44 DIREITOS DE PROPRIEDADE INTELECTUAL E DIREITOS AUTORAIS DA SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO

44.1 Em conformidade com a IN04/2014, o Art. 18, inciso I letra i e inciso II letra i, define-se a seguir quais serão os direitos a propriedade intelectual que caberá à administração, fruto do fornecimento pertinente a esta contratação, a saber:

44.1.1 Não se aplicará direito de propriedade intelectual à administração sobre o código fonte, visto que a execução dos serviços não envolve desenvolvimento de software e/ou aplicativo.

44.1.2 Destaca-se que a administração pretende adquirir hardware e software prontos, onde não se aplicar-se-á o direito de propriedade intelectual.

44.1.3 Não se aplicará direito de propriedade intelectual à administração sobre a documentação original que acompanha a plataforma de hardware e software, visto que a execução do fornecimento não envolve desenvolvimento de software e/ou aplicativo e/ou manuais.

44.1.3.1 Se aplicará direito de propriedade intelectual à administração sobre toda e qualquer documentação fruto da execução dos serviços prestados, exceto para a citada anteriormente.

## 45 LOCAL DE ENTREGA E EXECUÇÃO DO OBJETO

45.1 A entrega, de produtos e serviços, deverá ser realizada, em dias úteis, em horário comercial, nos endereços descritos no Apêndice “M”.

## 46 REUNIÕES DE ALINHAMENTO

46.1 Deverá ser realizada reunião de alinhamento com o objetivo de identificar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e Apêndices, e esclarecer possíveis dúvidas acerca da execução dos serviços.

46.2 Deverão participar dessa reunião, no mínimo o Gestor do Contrato no Ibama e o Preposto da CONTRATADA.

46.3 A reunião realizar-se-á no Ibama em até 15 (quinze) dias úteis a contar da data de assinatura do Contrato, conforme agendamento efetuado pelo Gestor do Contrato no Ibama.

46.4 Nessa reunião a CONTRATADA deverá apresentar oficialmente seu Preposto, por meio de Ofício de designação.

46.5 Todos os entendimentos da reunião de alinhamento deverão constar da Ata de reunião a ser lavrada pelo Gestor do Contrato no Ibama e assinada por todos os participantes.

46.6 A CONTRATADA cumprirá as instruções complementares do Ibama quanto à execução e horário de realização do serviço, permanência e circulação de seu (s) técnico (s) nas dependências do Ibama.

## 47 PROPOSTA DE PREÇOS

47.1 A proposta da licitante deverá conter a composição clara e completa dos equipamentos ofertados, obedecida a mesma ordem constante deste documento, sem conter alternativas de preços, ou de qualquer outra condição que induza o julgamento a ter mais de um resultado.

47.2 Os preços ofertados devem incluir também todos os insumos necessários, mão de obra, impostos e taxas e todas as leis sociais incidentes na execução dos trabalhos.

47.3 A proposta deverá apresentar obrigatoriamente para cada item do escopo de fornecimento:

47.3.1 Nome Fabricante e/ou Marca;

47.3.2 Modelo do Produto ofertado;

47.3.3 País de Origem do Produto;

47.3.4 Códigos (Part Number) de identificação de cada elemento que compõem o conjunto ofertado para cada unidade do escopo de fornecimento;

47.3.5 Quantidades de cada elemento que compõem o conjunto de elementos ofertado para cada unidade do escopo de fornecimento.

47.4 A licitante vencedora deverá apresentar planilha de preços, discriminando os valores total e unitário dos serviços contratados.

47.5 Para comprovação das características do objeto constante deste documento, a licitante deverá:

47.5.1 Apresentar, junto a sua proposta comercial, documentação comprobatória do atendimento de todos os requisitos do Apêndice "A";

47.5.2 Apresentar comprovação de que os produtos ofertados são de origem comprovada e que possuem garantia do fabricante no território nacional;

47.5.3 Apresentar documentação técnica (manuais, catálogos oficiais do fabricante) comprovando o pleno atendimento a todos os requisitos técnicos, por meio de apresentação de uma planilha ponto-a-ponto, com indicação de nome do documento e página que comprova o atendimento. Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante, exceto quando explicitamente permitido em algum item específico;

47.5.4 A CONTRATANTE poderá a qualquer momento realizar diligência para comprovação da veracidade de qualquer documento apresentado.

47.6 A proposta da licitante deverá estar integralmente preenchida, discriminando os valores unitários e totais dos bens objeto deste documento, em conformidade com o modelo constante.

## 48 FORMA DE PAGAMENTO

48.1 O pagamento será efetuado pela Contratante no prazo de 30 (trinta) dias, contados da apresentação da Nota Fiscal/Fatura contendo o detalhamento dos serviços executados e os materiais empregados, através de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado.

48.2 Os pagamentos decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 24 da Lei 8.666, de 1993, deverão ser efetuados no prazo de até 5 (cinco) dias úteis, contados da data da apresentação da Nota Fiscal/Fatura, nos termos do art. 5º, § 3º, da Lei nº 8.666, de 1993.

48.3 A apresentação da Nota Fiscal/Fatura deverá ocorrer no prazo de 3 (três) dias, contado da data final do período de adimplemento da parcela da contratação a que aquela se referir.

48.4 O pagamento somente será autorizado depois de efetuado o “atesto” pelo servidor competente, condicionado este ato à verificação da conformidade da Nota Fiscal/Fatura apresentada em relação aos serviços efetivamente prestados e aos materiais empregados.

48.5 Havendo erro na apresentação da Nota Fiscal/Fatura ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

48.6 Nos termos do artigo 36, § 6°, da Instrução Normativa STI/MPOG n° 02, de 2008, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

48.6.1 não produziu os resultados acordados;

48.6.2 deixou de executar as atividades contratadas, ou não as executou com a qualidade mínima exigida;

48.6.3 deixou de utilizar os materiais e recursos humanos exigidos para a execução do serviço, ou utilizou-os com qualidade ou quantidade inferior à demandada.

48.7 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

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

48.9 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.

48.10 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.

48.11 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.

48.12 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.

48.13 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.

48.14 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

48.15 A Contratada regularmente optante pelo Simples Nacional não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na LC.

48.16 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:

48.16.1 EM = I x N x VP, sendo:

48.16.2 EM = Encargos moratórios;

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

48.16.4 VP = Valor da parcela a ser paga.

48.16.5 I = Índice de compensação financeira = 0,00016438, assim apurado:

48.16.6 I = 6% (ao ano) / 365 (dias ano) / 100

## 49 CRONOGRAMA FÍSICO-FINANCEIRO

| CRONOGRAMA DE EVENTOS E PAGAMENTOS | | | |
|---|---|---|---|
| **Item** | **Evento** | **Data** | **% a pagar** |
| **Todos os Itens** | | | |
| 1 | Assinatura do contrato. | Dia X | 0% |
| 2 | Reunião Inicial – Plano de Inserção | Dia $D_1$, sendo $D_1$ conforme demanda da CONTRATANTE | 0% |
| **CRONOGRAMA DE EVENTOS E PAGAMENTO ITEM 01** | | | |
| 3 | Emissão OS – Ordem de Serviço | Dia $D_2$, sendo $D_2$ conforme demanda da CONTRATANTE | 0% |
| 4 | Entrega dos plano de trabalho e cronograma de atividades; | $D_2$ + 60 dias | 0% |

| | | | |
|---|---|---|---|
| 5 | Entrega dos produtos ( Hardware, Software ou licenças) e emissão do **Termo de Recebimento Provisório – TRP** de Produtos. | $D_{2a} = D_2$ + 45 dias úteis | 85% |
| 6 | Execução dos serviços de instalação, ativação ou atualização, conforme cada caso, e emissão do **Termo de Recebimento Provisório – TRP** de Serviço. | $D_{2a}$ + 60 dias | 15% |

## 50 INTERAÇÃO ENTRE CONTRATANTE E CONTRATADA

50.1 A CONTRATADA deverá propor um Plano de Comunicação com o Ibama, por meio de documentação, a qual deverá ser aprovada e aceita pelo Gestor do Contrato.

50.2 São mecanismos formais de comunicação entre a CONTRATADA e a CONTRATANTE:

50.2.1 **E-mails**: forma rápida de comunicação para tratar de informações pouco críticas;

50.2.2 **Ofícios**: Comunicação para tratar de assuntos gerais;

50.2.3 **OF - Ordem de Fornecimento**: elaborada, por demanda, pela CONTRATANTE e encaminhada à CONTRATADA;

50.2.4 **Termo de Aceite Provisório**: termo elaborado pela CONTRATANTE e encaminhado à CONTRATADA;

50.2.5 **Termo de Aceite Definitivo**: termo elaborado pela CONTRATANTE e encaminhado à CONTRATADA.

50.3 Toda a comunicação entre a Administração Pública e a CONTRATADA deverá ser sempre formal como regra, exceto em casos excepcionais que justifiquem outro canal de comunicação.

## 51 VÍNCULO EMPREGATÍCIO

51.1 A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta, e não há dedicação de mão de obra exclusiva.

51.2 Os profissionais e representantes da CONTRATADA não terão nenhum vínculo empregatício com o Ibama, correndo por conta exclusiva da CONTRATADA, todas as obrigações decorrentes da legislação trabalhista, previdenciária, infortunística do trabalho, fiscal, comercial e outras correlatas, as quais a CONTRATADA se obriga a saldar na época devida.

## 52 DA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIOS

52.1 É vedada a participação de empresas consorciadas, um vez que não há no sistema legal regedor das licitações imposição da aceitabilidade de consórcio, ficando, em razão disso, a Administração Pública, e no exercício de seu poder discricionário, com liberdade de promover referida limitação, desde que, é claro, o faça atento ao princípio constitucional e administrativo da razoabilidade. Admitir consórcio é repartir serviços que devem ter sua execução sistêmica e, ainda correr o risco de obter ao final um serviço sem unidade o que fatalmente ocasionará prejuízos à Administração.

52.2 Assim, a Administração Pública ao vedar a participação de consórcio procura manter a unidade do sistema, eis que o TR, da forma como foi concebido demonstra a existência de uma unidade conceitual que perpassa todo o projeto. Tal integração de conceitos se verifica não só entre suas etapas, como também nos produtos/serviços previstos em cada etapa. Isto porque cada produto/serviço solicitado representa uma preparação para que o produto/serviço subsequente possa ser compreendido e elaborado. Vale dizer que somente a empresa que estiver envolvida e for responsável pela totalidade do objeto será conhecedora, de forma suficiente, de todas as questões pertinentes, estando apta a apresentar os produtos/serviços de forma encadeada.

## 53 VIGÊNCIA DO CONTRATO

53.1 O **CONTRATO** terá vigência de 36 (trinta e seis) meses a contar da data de sua assinatura, podendo ser prorrogado por iguais e sucessivos períodos até o limite de 60 (sessenta) meses, conforme inciso II, art. 57 da Lei nº 8.666/93.

53.2 O Contratado deverá sujeitar-se aos acréscimos e supressões contratuais estabelecidos na forma do Art. 65 da Lei n. 8.666/93.

## 54 GARANTIA DE EXECUÇÃO

54.1 O adjudicatário, no prazo de 5 (cinco dias) após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 3% (três por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Edital, conforme disposto no art. 56 da Lei nº 8.666, de 1993, desde que cumpridas as obrigações contratuais.

54.2 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, até o máximo de 2% (dois por cento).

54.3 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, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666, de 1993;

54.4 A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de mais 3 (três) meses após o término da vigência contratual.

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

54.5.1 prejuízos advindos do não cumprimento do objeto do contrato;

54.5.2 prejuízos diretos causados à Administração decorrentes de culpa ou dolo durante a execução do contrato;

54.5.3 multas moratórias e punitivas aplicadas pela Administração à contratada; e

54.5.4 obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela contratada, quando couber.

54.6 A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados no item anterior, mencionados no art. 19, XIX, b da IN STI/MPOG 02/2008, observada a legislação que rege a matéria.

54.7 A garantia em dinheiro deverá ser efetuada em favor da Contratante, em conta específica na Caixa Econômica Federal, com correção monetária.

54.8 No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

54.9 Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a Contratada obriga-se a fazer a respectiva reposição no prazo máximo de 2 (dois) dias úteis, contados da data em que for notificada.

54.10 A Contratante executará a garantia na forma prevista na legislação que rege a matéria.

54.11 Será considerada extinta a garantia:

54.11.1 Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração da Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato;

54.11.2 No prazo de três meses após o término da vigência, caso a Contratante não comunique a ocorrência de sinistros.

## 55 REEQUILÍBRIO ECONÔMICO-FINANCEIRO

55.1 Com vistas a manutenção do equilíbrio econômico-financeiro do Contrato, poderá ser promovida revisão do preço contratual, desde que eventuais solicitações nesse sentido estejam acompanhadas de comprovação da superveniência de fatos imprevisíveis ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, configurando álea econômica extraordinária e extracontratual, bem como de demonstração analítica de seu impacto nos custos do Contrato, nos termos do disposto no art. 65, inciso II, alínea “d”, da lei nº 8.666/93.

## 56 DO REAJUSTE

56.1 O valor do contrato poderá ser reajustado pelo Índice Geral de Preços de Mercado – IGP-M (FGV) ou outro índice oficial que vier a substituí-lo, desde que observado o interregno mínimo de 12 (doze) meses, contados da assinatura do contrato.

56.2 O reajuste somente será concedido após análise pelo setor competente e mediante motivação e comprovação, por parte da CONTRATADA.

56.3 A utilização do Índice Geral de Preços de Mercado – IGP-M (FGV) se justifica por se tratar de serviço continuo sem dedicação exclusiva de mão-de-obra e ainda visando à recomposição dos valores contratados em vista dos efeitos inflacionários, além de ser mais vantajoso para a Administração

## 57 LEGISLAÇÃO APLICÁVEL

57.1 A presente contratação será realizada por meio de processo licitatório, na modalidade de Pregão Eletrônico, observando os dispositivos legais, notadamente os princípios da (o):

57.1.1 Lei nº 8.248, de 23 de outubro de 1991 - Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências;

57.1.2 Lei nº 8.666, de 21 de junho de 1993 - Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências;

57.1.3 Lei nº 10.520, de 17 de julho de 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;

57.1.4 Decreto nº 3.722, de 9 de janeiro de 2001 - Regulamenta o art. 34 da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre o Sistema de Cadastramento Unificado de Fornecedores - SICAF;

57.1.5 Decreto nº 7.174, de 12 de maio de 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;

57.1.6 Decreto nº 7.746, de 5 de junho de 2012 - Regulamenta o art. 3º da Lei nº 8.666, de 21 de junho de 1993, para estabelecer critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável nas contratações realizadas pela administração pública federal, e institui a Comissão Interministerial de Sustentabilidade na Administração Pública – CISAP;

57.1.7 Instrução Normativa STI/MPOG nº 02, de 30 de abril de 2008 - Dispõe sobre regras e diretrizes para a contratação de serviços, continuados ou não;

57.1.8 Instrução Normativa STI/MPOG nº 1, de 19 de janeiro de 2010 - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

57.1.9 Instrução Normativa STI/MPOG nº 4, de 11 de setembro de 2014 - Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal. (Redação dada pela Instrução Normativa N° 2, de 12 de janeiro de 2015);

57.1.10 Instrução Normativa STI/MPOG nº 6, de 23 de dezembro de 2013 - Altera a Instrução Normativa nº 2, de 30 de abril de 2008, e seus Anexos I, III, IV, V e VII e inclui o Anexo VIII;

57.1.11 Decreto nº 5.450/2005: Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.

57.1.12 Lei nº 8.248/1991 - Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.

57.1.13 Decreto nº 8.184/2014 - Estabelece a aplicação de margem de preferência em licitações realizadas no âmbito da administração pública federal para aquisição de equipamentos de tecnologia da informação e comunicação, para fins do disposto no art. 3º da Lei nº 8.666, de 21 de junho de 1993.

57.1.14 PORTARIA Nº 20, DE 14 DE JUNHO DE 2016 - Dispõe sobre orientações para contratação de soluções de Tecnologia da Informação no âmbito da Administração Pública Federal direta, autárquica e fundacional e dá outras providências.

57.1.15 e demais legislações pertinentes e, ainda, pelo estabelecido no presente documento e seus anexos.

## 58 DA APLICABILIDADE DO DECRETO 7.174/2010, ART. 3º

58.1 Inciso I do Decreto 7.174/2010

58.1.1 Constam no apêndice "A" as especificações técnicas a serem consideradas na licitação;

58.2 Inciso II do Decreto 7.174/2010

58.2.1 ***Segurança para o usuário e instalações:*** Não se aplica ao objeto da pretendida contratação;

58.2.2 ***Compatibilidade eletromagnética*****:** Constam no apêndice "A" as especificações técnicas a serem consideradas na licitação;

58.2.3 ***Consumo de energia*****:** Não se aplica ao objeto da pretendida contratação.

58.3 Inciso III do Decreto 7.174/2010

58.3.1 **A contratada deverá comprovar**, se cabível ao objeto, a origem dos bens importados ofertados e a quitação dos tributos referentes à importação, no momento da entrega do objeto deste Termo de Referência, sob pena de rescisão contratual, multa e responsabilização da contratada pelos danos eventualmente causados.

58.4 Inciso IV do Decreto 7.174/2010

58.4.1 A metodologia de aferição e o índice de desempenho exigido estão especificados nos respectivos itens da especificação da solução disponível no **APENDICE "A"** deste Termo de Referência, bem como através dos requisitos do **Acordo de Nível de Serviço**.

## 59 DISPOSIÇÕES GERAIS

59.1 O Pregoeiro responsável pelo certame reserva-se o direito de solicitar da LICITANTE, em qualquer tempo, no curso da licitação, quaisquer esclarecimentos sobre documentos já entregues, fixando-lhe prazo para atendimento;

59.2 A falta de qualquer dos documentos exigidos no edital implicará inabilitação da LICITANTE, sendo vedada a concessão de prazo para complementação da documentação exigida para a habilitação, salvo motivo devidamente justificado e aceito pelo pregoeiro.

59.3 Integram este termo de referência os seguintes apêndices:

| Apêndice | Descrição |
|---|---|
| Apêndice "A" | Especificações Mínimas e Obrigatórias |
| Apêndice "B" | Condições Gerais de Execução dos Serviços de Garantia e Suporte |
| Apêndice "C" | Procedimento de Avaliação das Amostras |
| Apêndice "D" | Modelo de Declaração de Vistoria |
| Apêndice "E" | Modelo de Declaração de Recusa de Vistoria |
| Apêndice "F" | Modelo de Proposta de Preços |
| Apêndice "G" | Modelo de OF - Ordem de Fornecimento |
| Apêndice "H" | Termo de Recebimento Provisório |
| Apêndice "I" | Termo de Recebimento Definitivo |
| Apêndice "J" | Termo de Confidencialidade da Informação |
| Apêndice "K" | Termo de Ciência |
| Apêndice "L" | Termo de Encerramento do Contrato |
| Apêndice "M" | Relação de Endereços das Localidades |
| Apêndice "N" | Termo de Execução de Capacitação Técnica |
| Apêndice "O" | Termo de Recebimento POSIC |
| Apêndice "P" | Formulário de Avaliação de Capacitação Técnica |
| Apêndice "Q" | Lista de Presença |
| Apêndice "R" | Estimativa de Preços |
| Apêndice "S" | Memorial de Cálculo |

Em atendimento ao Art. 14, § 6º da Instrução Normativa SLTI/MP nº 04/2014, a equipe de planejamento da contratação **aprova** o Termo de Referência e encaminha a Autoridade Competente para a devida aprovação, nas condições e quantidades definidas, por se mostrarem adequadas ao interesse da Administração.

**INTEGRANTE REQUISITANTE**

**TELVIO MARTINS DE MELLO**
**SIAPE: 2425456**

**INTEGRANTE TÉCNICO**

**MARCUS THADEU DE OLIVEIRA SILVA**
**SIAPE: 1108302**

**INTEGRANTE ADMINISTRATIVO**

**SUÉLIO LUIGI BARBOSA DE MORAIS**
**SIAPE: 2163423**

## APÊNDICE "A"

## ESPECIFICAÇÕES MÍNIMAS E OBRIGATÓRIAS

Neste apêndice estão especificados os requisitos mínimos e obrigatórios para o item do escopo de fornecimento, onde a licitante deverá apresentar documentação comprobatória do atendimento de todos os requisitos, bem como deve ainda:

- Apresentar garantias de que os produtos ofertados são de origem comprovada e que possuem garantia do fabricante no território nacional;

- Apresentar documentação técnica (manuais, catálogos oficiais do fabricante) comprovando o pleno atendimento a todos os requisitos técnicos, por meio de apresentação de uma planilha ponto a ponto, com indicação de nome do documento e página que comprova o atendimento. Não será aceita comprovação por carta do fabricante ou distribuidor ou da licitante;

- A CONTRATANTE poderá a qualquer momento realizar diligência para comprovação da veracidade de qualquer documento apresentado.

## LOTE 01

### ITEM 1 - SOLUÇÃO DE SEGURANÇA (NGFW) COM SUBSCRIÇÃO E PRODUTO

### ESPECIFICAÇÕES BÁSICAS

**1. Descrição**

1.1. Aquisição de solução de Segurança de rede, incluindo subscrição e produto, com características de Next Generation Firewall (NGFW) para segurança de informação perimetral que inclui filtro de pacote, controle de aplicação, administração de largura de banda (QoS), VPN IPSec e SSL, IPS, prevenção contra ameaças de vírus, spywares e malwares "Zero Day", Filtro de URL, bem como controle de transmissão de dados e acesso a internet compondo uma plataforma de segurança integrada e robusta;

1.2. Por plataforma de segurança entende-se hardware e software integrados do tipo appliance.

**2. CAPACIDADE E QUANTIDADES**

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

2.1.1. Throughput de 17 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

2.1.2. Throughput de 8.5 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;

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

2.1.4. 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);

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

2.1.6. Suporte a, no mínimo, 3.800.000 de conexões simultâneas;

2.1.7. Suporte a, no mínimo, 110.000 novas conexões HTTP por segundo;

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

2.1.9. Cooler hot-swappble;

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

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

2.1.12. No mínimo, 04 (quatro) interfaces de rede 1 Gbps em portas cobre;

2.1.13. No mínimo, 08 (oito) interfaces de rede 1 Gbps SFP;

2.1.14. No mínimo, 08 (oito) interfaces de rede 10 Gbps SFP+;

2.1.15. No mínimo, 04 (quatro) interfaces de rede 40 Gbps QSFP+;

2.1.16. 2 (duas) Gbps interfaces dedicadas para alta disponibilidade sendo pelo menos uma do tipo 40 Gbps QSFP+;

2.1.17. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

2.1.18. 1 (uma) interface do tipo console ou similar;

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

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

2.1.21. Estar licenciada para ou suportar sem o uso de licença, 3.000 (três mil) túneis de VPN IPSEC simultâneos;

2.2. 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;

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

2.4. 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;

2.5. A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;

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

**CARACTERÍSTICAS GERAIS**

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

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

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

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

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

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

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

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

2.14.1. Suporte a 4094 VLAN Tags 802.1q;
2.14.2. Agregação de links 802.3ad e LACP;
2.14.3. Policy based routing ou policy based forwarding;
2.14.4. Roteamento multicast (PIM-SM);
2.14.5. DHCP Relay;
2.14.6. DHCP Server;
2.14.7. Jumbo Frames;
2.14.8. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;

2.15. Suportar sub-interfaces ethernet logicas;

2.15.1. Suporte a, no mínimo, 15 (quinze) roteadores virtuais na mesma instância de firewall;

2.16. 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;

2.17. Deve suportar os seguintes tipos de NAT:

2.17.1. Nat dinâmico (Many-to-1);
2.17.2. Nat dinâmico (Many-to-Many);
2.17.3. Nat estático (1-to-1);
2.17.4. NAT estático (Many-to-Many);
2.17.5. Nat estático bidirecional 1-to-1;
2.17.6. Tradução de porta (PAT);
2.17.7. NAT de Origem;
2.17.8. NAT de Destino;

2.17.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
2.17.10. Deve implementar Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;

2.18. Deve implementar o protocolo ECMP;
2.18.1. Deve implementar balanceamento de link por hash do IP de origem;
2.18.2. Deve implementar balanceamento de link por hash do IP de origem e destino;
2.18.3. Deve implementar balanceamento de link através do método round-robin;
2.18.4. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quarto links;
2.18.5. Deve implementar balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
2.18.6. Deve implementar balanceamento de link através de políticas por aplicação e porta de destino;
2.18.7. Deve implementar o protocolo Link Layer Dicovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
2.18.8. Enviar log para sistemas de monitoração externos, simultaneamente;
2.18.9. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
2.18.10. Deve permitir configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
2.18.11. Proteção contra anti-spoofing;
2.18.12. Deve permitir bloquear sessoes TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
2.18.13. Dever permitir bloquear conexões que contenham dados no payload de pacotes TCP-SYN e SYN-ACK durante o three-way handshake;
2.18.14. Deve exibir nos logs de tráfego o motivo para o término da sessão no firewall, incluindo sessões finalizadas onde houver de-criptografia de SSL e SSH;
2.18.15. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
2.18.16. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
2.18.17. Suportar a OSPF *graceful restart*;
2.18.18. Deve suportar o protocolo MP-BGP (Multiprotocol BGP) permitindo que o firewall possa anunciar rotas multicast para IPv4 e rotas unicast para IPv6;
2.18.19. 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;
2.18.20. 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);

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

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

2.18.20.3. 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;

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

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

2.19.1. Em modo transparente;

2.19.2. Em layer 3;

2.20. A configuração em alta disponibilidade deve sincronizar:

2.20.1. Sessões;

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

2.20.3. Certificados de-criptografados;

2.20.4. Associações de Segurança das VPNs;

2.20.5. Tabelas FIB;

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

2.21. 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 FIREWALL**

2.22. Deverá suportar controles por zona de segurança.

2.23. Controles de políticas por porta e protocolo.

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

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

2.26. 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;

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

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

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

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

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

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

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

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

2.33. 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;

2.34. 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);

2.34.1. 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 o firewall, quanto para as soluções de análise.

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

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

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

2.38. Suporte a objetos e regras IPV6.

2.39. Suporte a objetos e regras multicast.

2.40. 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;

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

**CONTROLE DE APLICAÇÕES**

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

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

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

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

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

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

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

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

2.42.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

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

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

2.42.11. Atualizar a base de assinaturas de aplicações automaticamente;

2.42.12. Reconhecer aplicações em IPv6;

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

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

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

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

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

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

2.42.19. 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:

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

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

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

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

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

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

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

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

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

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

2.42.27.2. Nível de risco da aplicação.

2.42.27.3. Categoria e sub-categoria de aplicações.

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

**PREVENÇÃO DE AMEAÇAS**

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

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

2.45. 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.

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

2.47. 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;

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

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

2.50. 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.

2.51. Deve permitir o bloqueio de vulnerabilidades.

2.52. Deve permitir o bloqueio de exploits conhecidos.

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

2.54. Deve suportar a inspeção e criação de regras de proteção de DOS e QOS para o conteúdo de tráfego tunelado pelo protocolo GRE;

2.55. Deverá possuir os seguintes mecanismos de inspeção de IPS:
- 2.55.1. Análise de padrões de estado de conexões;
- 2.55.2. Análise de decodificação de protocolo;
- 2.55.3. Análise para detecção de anomalias de protocolo;
- 2.55.4. Análise heurística;

2.55.5. IP Defragmentation;
2.55.6. Remontagem de pacotes de TCP;
2.55.7. Bloqueio de pacotes malformados.

2.56. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMP flood, UDP flood, etc;

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

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

2.59. 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;

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

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

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

2.63. 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;

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

2.65. 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;

2.66. Suportar bloqueio de arquivos por tipo;

2.67. Identificar e bloquear comunicação com botnets;

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

2.69. Deve suportar referencia cruzada com CVE;

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

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

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

2.73. 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;

2.74. 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;

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

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

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

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

2.79. Rastreamento de vírus em pdf.

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

2.81. 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**

2.82. 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;

2.83. 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;

2.84. 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;

2.85. 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.;

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

2.87. 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);

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

2.89. 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;

2.90. 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;

2.91. 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;

2.92. 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);

2.93. 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;

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

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

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

2.97. 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.

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

2.99. 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;

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

**FILTRO DE URL**

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

2.102. 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);

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

2.102.2. 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.

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

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

2.102.5. 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;

2.102.6. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

2.102.7. Possui pelo menos 60 categorias de URLs;

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

2.102.9. Suporta a criação categorias de URLs customizadas;

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

2.102.11. Permite a customização de página de bloqueio;

2.102.12. 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;

2.102.13. 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;

2.102.14. 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);

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

2.102.16. 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**

2.103. 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;

2.104. 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;

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

2.106. 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;

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

2.107.1.1. 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;

2.108. 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);

2.109. Suporte a autenticação Kerberos;

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

2.111. 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;

2.112. 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;

2.113. 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;

2.114. 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;

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

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

**QOS**

2.117. 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.

2.118. Suportar a criação de políticas de QoS por:
- 2.118.1. Endereço de origem
- 2.118.2. Endereço de destino
- 2.118.3. Por usuário e grupo do LDAP/AD.
- 2.118.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- 2.118.5. Por porta;

2.119. O QoS deve possibilitar a definição de classes por:
- 2.119.1. Banda Garantida
- 2.119.2. Banda Máxima
- 2.119.3. Fila de Prioridade.

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

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

2.122. 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);

2.123. Disponibilizar estatísticas RealTime para classes de QoS.

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

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

**FILTRO DE DADOS**

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

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

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

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

2.130. 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;

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

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

**Geo-localização**

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

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

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

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

**VPN**

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

2.138. Suportar IPSec VPN;

2.139. Suportar SSL VPN;

2.140. A VPN IPSEc deve suportar:
- 2.140.1.DES e 3DES;
- 2.140.2.Autenticação MD5 e SHA-1;
- 2.140.3.Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
- 2.140.4.Algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.140.5.AES 128, 192 e 256 (Advanced Encryption Standard)
- 2.140.6.Autenticação via certificado IKE PKI.

2.141. Deve possuir interoperabilidade com os seguintes fabricantes:
- 2.141.1.Cisco;
- 2.141.2.Checkpoint;
- 2.141.3.Juniper;
- 2.141.4.Palo Alto Networks;
- 2.141.5.Fortinet;
- 2.141.6.Sonic Wall;

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

2.143. A VPN SSL deve suportar:

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

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

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

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

2.143.5. 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;

2.143.6. 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;

2.143.7. Atribuição de DNS nos clientes remotos de VPN;

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

2.143.9. 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;

2.143.10. Deve possuir lista de bloqueio para dispositivos que forem reportados com roubado ou perdido pelo usuário;

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

2.143.12. 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;

2.143.13. 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;

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

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

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

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

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

2.143.19. 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;

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

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

2.143.22. 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;

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

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

2.143.24.1. Antes do usuário autenticar na estação;
2.143.24.2. Após autenticação do usuário na estação;
2.143.24.3. Sob demanda do usuário;

2.143.25. Deverá Manter uma conexão segura com o portal durante a sessão.

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

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

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

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

**CONSOLE DE GERÊNCIA E MONITORAÇÃO**

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

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

2.146. 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;

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

2.148. O gerenciamento deve permitir/possuir:
- 2.148.1. Criação e administração de políticas de firewall e controle de aplicação;
- 2.148.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
- 2.148.3. Criação e administração de políticas de Filtro de URL;
- 2.148.4. Monitoração de logs;
- 2.148.5. Ferramentas de investigação de logs;
- 2.148.6. Debugging;
- 2.148.7. Captura de pacotes.

2.149. Acesso concorrente de administradores;

2.150. 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;

2.151. 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.

2.152. 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;

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

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

2.155. 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;

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

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

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

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

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

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

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

2.163. Criação de regras com data de expiração;

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

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

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

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

2.168. Validação de regras antes da aplicação;

2.169. 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.

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

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

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

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

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

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

2.174. 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;

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

2.176. 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;

2.177. 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;

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

2.179. 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.

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

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

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

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

2.184. 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;

2.185. 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;

2.186. Deve ser possível exportar os logs em CSV;

2.187. 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.

2.188. Rotação do log;

2.189. 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;

2.190. 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;

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

2.191.1. Situação do dispositivo e do cluster;

2.191.2. Principais aplicações;

2.191.3. Principais aplicações por risco;

2.191.4. Administradores autenticados na gerência da plataforma de segurança;

2.191.5. Número de sessões simultâneas;

2.191.6. Status das interfaces;

2.191.7. Uso de CPU;

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

2.192.1. Resumo gráfico de aplicações utilizadas;

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

2.192.3. Principais aplicações por taxa de transferência de bytes;
2.192.4. Principais hosts por número de ameaças identificadas;

2.192.5. 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;

2.192.6. Deve permitir a criação de relatórios personalizados;

2.193. 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;

2.194. Gerar alertas automáticos via:
2.194.1. Email;
2.194.2. SNMP;
2.194.3. Syslog;

2.195. 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.

## CONDIÇÕES GERAIS DE EXECUÇÃO DOS SERVIÇOS DE GARANTIA E SUPORTE

### 1 SERVIÇOS DE GARANTIA E SUPORTE

1.1 Os serviços poderão ser prestados pela CONTRATADA ou por representante indicada pela CONTRATADA ou pelo fabricante da solução, sem prejuízo a responsabilidade integral da CONTRATADA quanto aos atendimento dos níveis de serviço;

1.2 Entende-se por "Garantia" ou ""Suporte" ou "Manutenção", doravante denominada unicamente como "Garantia", toda atividade do tipo "corretiva" não periódica que

variavelmente poderá ocorrer, durante todo o período de garantia. A mesma possui suas causas em falhas e erros no Software/Hardware e trata da correção dos problemas atuais e não iminentes de fabricação dos mesmos. Esta "Garantia" inclui os procedimentos destinados a recolocar em perfeito estado de operação os serviços e produtos ofertados, tais como:

1.2.1 **Do hardware**: desinstalação, reconfiguração ou reinstalação decorrente de falhas de fabricação no hardware, fornecimento de peças de reposição, substituição de hardware defeituoso por defeito de fabricação, atualização da versão de drivers e firmwares, correção de defeitos de fabricação, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados

1.2.2 **Do software**: desinstalação, reconfiguração ou reinstalação decorrente de falhas de desenvolvimento do software, atualização da versão de software, correção de defeitos de desenvolvimento do software, de acordo com os manuais e as normas técnicas específicas do fabricante para os recursos utilizados;

1.2.2.1 **Quanto às atualizações pertinentes aos softwares**: Entende-se como "atualização" o provimento de toda e qualquer evolução de software, incluindo correções, "patches", "fixes", "updates", "service packs", novas "releases", "versions", "builds", "upgrades", englobando inclusive versões não sucessivas, nos casos em que a solicitação de atualização de tais versões ocorra durante o período de garantia do contrato.

1.3 A CONTRATADA fornecerá e aplicará pacotes de correção, em data e horário a serem definidos pela CONTRATANTE, sempre que forem encontradas falhas de laboratório (bugs) ou falhas comprovadas de segurança em software ou firmware dos aparelhos que integrem o objeto do contrato.

1.3.1 O atendimento deste requisito está condicionado a liberação pelo fabricante dos pacotes de correção e/ou novas versões de software.

1.4 É facultado a CONTRATADA a execução, ao seu planejamento e disponibilidade, de "Garantia" do tipo "preventiva" que pela sua natureza reduza a incidência de problemas que possam gerar "Garantia" do tipo "corretiva". As manutenções do tipo "preventiva" não podem gerar custos a CONTRATANTE.

1.5 A manutenção técnica do tipo "corretiva" será realizada sempre que solicitada pelo CONTRATANTE por meio da abertura de chamado técnico diretamente à empresa CONTRATADA (ou a outra informada pela CONTRATADA) via telefone (com número do tipo "0800" caso a Central de Atendimento esteja fora de Brasília-DF) ou Internet ou e-mail ou fac-símile ou outra forma de contato;

1.6 Os serviços de "Garantia" incluem:

1.6.1 Solução de problemas relativos à indisponibilidade da solução decorrentes de problemas de fabricação e desenvolvimento;

1.6.2 Solução de falhas ou defeitos no funcionamento, incluindo a instalação de arquivos para correção dos erros;

1.6.3 Esclarecimento de dúvidas sobre o funcionamento e operação da solução;

1.6.4 Instalação de novas versões ou atualizações e patches;

1.7 A CONTRATADA deve disponibilizar a central atendimento 8 horas por dia, 5 dias da semana (de segunda a sexta-feira, exceto feriados) e equipe com conhecimentos sólidos no funcionamento e operação da solução de gestão.

1.8 O serviço de "Garantia" deve disponibilizar o seguintes tipos de atendimento:

1.8.1 **Nível I - Atendimento Telefônico (Help Desk)**: chamados abertos através de ligação telefônica ou e-mail ou outro forma de contato, em regime de 8x5: 8 horas por dia, 5 dias da semana (de segunda a sexta-feira, exceto feriado). Esse serviço deve atender demandas dos usuários referentes ao funcionamento da solução, que decorram de problemas de funcionamento.

1.8.2 **Nível II - Atendimento Remoto**: atendimento remoto de chamados de suporte técnico através de tecnologia disponibilizada pela CONTRATANTE, mediante prévia autorização e seguindo os padrões de segurança da CONTRATANTE, objetivando análise e solução remota dos problemas apresentados.

1.8.3 **Nível III - Atendimento Presencial (On-Site)**: atendimentos técnicos realizados nas dependências do CONTRATANTE, através de visita de técnico especializado, com a finalidade de resolver demandas abertas no Help Desk e não solucionadas pelo Atendimento Telefônico e/ou Remoto.

1.9 Toda "Garantia" deve ser solicitada inicialmente via Help Desk (Nível I), ficando a transferência do atendimento para o Atendimento Remoto (Nível II) condicionado à autorização da CONTRATANTE.

1.10 Toda "Garanita" solicitada inicialmente via Help Desk (Nível I), deve ser transferido para o Atendimento Presencial (Nível III) quando o atendimento do Help Desk não for suficiente para solução do problema sem a intervenção presencial de um técnico.

1.11 Os prazos para a prestação dos serviços devem garantir a observância ao atendimento do seguinte **Acordo de Níveis de Serviços (ANS)** e sua **SEVERIDADE**:

1.11.1 **SEVERIDADE URGENTE** – Solução totalmente inoperante.

1.11.1.1 Prazo máximo de início de atendimento de até 04 horas úteis contadas a partir do horário de abertura do chamado;

1.11.1.2 Prazo máximo de resolução do problema de até 24 horas úteis contadas a partir do início do atendimento.

1.11.2 **SEVERIDADE IMPORTANTE** – Solução parcialmente inoperante – Necessidade de suporte na solução com a necessidade de interrupção de funcionamento da solução.

1.11.2.1 Prazo máximo de início de atendimento de até 24 horas úteis contadas a partir do horário de abertura do chamado;

1.11.2.2 Prazo máximo de resolução do problema de até 48 horas úteis contadas a partir do início do atendimento.

1.11.3 **SEVERIDADE NORMAL** – Solução não inoperante mas com problema de funcionamento – Necessidade de suporte na solução sem a necessidade de interrupção de funcionamento da solução.

1.11.3.1 Prazo máximo de início de atendimento de até 48 horas úteis contadas a partir do horário de abertura do chamado;

1.11.3.2 Prazo máximo de resolução do problema de até 96 horas úteis contadas a partir do início do atendimento.

1.11.4 **SEVERIDADE EXTERNO** – Solução inoperante, de forma parcial ou total, fruto de falha de elemento de hardware e/ou software não fornecido pela CONTRATADA. Neste caso, ficam suspensos todos os prazos de atendimento até que a CONTRATANTE resolva os problemas externos que provocam a inoperância da solução. Após a CONTRATANTE disponibilizar o ambiente de forma estável para a reativação da solução, a CONTRATADA realizará avaliação da extensão do dano a solução e as partes definirão em comum acordo o prazo para a reativação da solução. Caso seja necessária a reinstalação da solução, a reinstalação será realizada através dos serviços compatíveis do "Catálogo de Serviços".

1.11.5 **SEVERIDADE INFORMAÇÃO** – Solicitações de informações diversas ou dúvidas sobre a solução.

1.11.5.1 Prazo máximo de resposta de até 10 dias úteis, contados a partir da data de abertura da ocorrência.

1.12 Um chamado técnico somente poderá ser fechado após a confirmação do responsável da CONTRATANTE e o término de atendimento dar-se-á com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado;

1.13 Na abertura de chamados técnicos, serão fornecidas informações, como Número de série (quando aplicável), anormalidade observada, nome do responsável pela solicitação do serviço e versão do software utilizada e **severidade** do chamado.

1.14 A **severidade** do chamado poderá ser reavaliada quando verificado que a mesma foi erroneamente aplicada, passando a contar no momento da reavaliação os novos prazos de atendimento e solução;

1.15 A CONTRATADA poderá solicitar a prorrogação de qualquer dos prazos para conclusão de atendimentos de chamados, desde que o faça antes do seu vencimento e devidamente justificado.

1.16 Os tempos de "início de atendimento" e "solução do problema" se aplicam para chamados com atendimento na cidade de Brasília – DF, onde para outras cidades, deve ser adicionado ao tempo de "início de atendimento" e de "solução do problema" os valores constantes no "Quadro de ajuste de tempos":

| QUADRO DE AJUSTE DE TEMPO | |
|---|---|
| Local de atendimento | Tempo adicional |
| Qualquer capital das unidades federativas do Brasil; | 08 horas úteis |
| Município distante da capital do estado em até 50 km; | 14 horas úteis |
| Município distante da capital do estado em até 150 km; | 20 horas úteis |
| Município distante da capital do estado em até 250 km; | 26 horas úteis |
| Município distante da capital do estado acima de 250 km; | 32 horas úteis |

# APÊNDICE "B"

# COMPOSIÇÃO DO CATÁLOGO DE SERVIÇOS

| A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|
| **Item** | **Descrição do Serviço** | **Evento** | **Quantidade de esforço em UST** | **Complexidade** | **Multiplicador da complexidade** | **Esforço p/ evento de serviço D X F** | **Quantidade estimada de ocorrências do evento por Ano** | **Esforço total estimado p/ ano em UST G x H** | **Prazo de início de execução - em dias** | **Prazo de execução após início - em dias** |
| | | | | | | | | | | |
| 01 | Reconfiguração FIREWALL | Reconfiguração | 16 | Baixa | 1 | 16 | 60 | **960** | 5 | 2 |
| 02 | Serviço de capacitação técnica individual | Capacitação | 24 | Média | 1,3 | 31,2 | 6 | **188** | 30 | 5 |
| | | | | | | | | | | |

## 1 DA DESCRIÇÃO DAS COLUNAS DA COMPOSIÇÃO DO CATÁLOGO DE SERVIÇOS

1.1 Item: Número sequencial dos itens de serviço do catálogo;

1.2 Descrição do Serviço: Descrição sucinta dos serviços do catálogo. Para verificar a descrição detalhada, vide item 2 deste apêndice.

1.3 Evento: Descreve o evento de serviço aplicada a cada item, para a qual será definida uma quantidade de esforço em UST por evento e um valor unitário de UST. Vide detalhamento:

1.3.1 Reconfiguração: Define o tipo do serviço, podendo ser reinstalação ou reconfiguração. Cada necessidade de reconfiguração gera um evento de serviço. Exemplo: Ser for necessário a reconfiguração 1 (um) Firewall, será emita OS para um evento, entretanto, se a necessidade for de reconfiguração de 2 (dois) Firewalls, será emita OS para dois eventos.

1.3.2 Capacitação: Define que a capacitação será solicitada por participante, ou seja, de forma individual. Para cada capacitação individual solicitada gerar-se-á um evento do respectivo serviço.

1.4 Quantidade de Esforço em UST: Define o esforço básico necessário a execução de um evento do serviço.

1.5 Complexidade: Define a complexidade de execução da tarefa e consequentemente define um multiplicador sobre o esforço.

1.5.1 Baixa: Envolve atividades de execução de rotinas já definidas ou desenvolvidas ou padronizadas.

1.5.2 Média: Envolve atividades de customização de rotinas existentes e serviços de capacitação de administração e operação da solução e apoio operacional.

1.5.3 Moderada: Envolve atividades de reconfiguração de elementos mais críticos e serviços de apoio operacional.

1.5.4 Alta: Envolve atividades de avaliação, análise e preparação de relatórios de mudanças de implementação, topologia, bem como definição de melhores práticas.

1.6 Multiplicador da Complexidade: É um fator, >= 1, aplicado sobre a "Quantidade de Esforço em UST". Isto permite aplicar o mesmo Valor em R$ de 1 UST a serviços de complexidade

diferenciada, que pode envolver profissionais de qualificação diferente, sem alterar o valor unitário em R$ da UST ofertada pela licitante vencedora.

1.7 Esforço p/ Evento de Serviço: Define o esforço total necessário para a execução de 1 (um) e evento do serviço, já aplicado o multiplicador de complexidade.

1.8 Quantidade estimada de ocorrências do evento p/ ano: Define a quantidade estimada de ocorrências do respectivo serviço por Ano;

1.9 Esforço total estimado p/ ano em UST: Define a quantidade total estimada de USTs por ano a serem contratadas para possível execução conforme demanda da CONTRATANTE. A quantidade total é resultado da multiplicação das colunas G x H , respectivamente, "Esforço p/ Evento de Serviço" x "Quantidade estimada de ocorrências do evento p/ ano".

1.10 Prazo de início de execução em dias: Prazo que a CONTRATADA possui para preparar o início da execução do respectivo item do catálogo de serviços.

1.11 Prazo de execução após início em dias: Prazo que a CONTRATADA possui para concluir a execução dos serviços após ter iniciado.

## 2 DESCRIÇÃO DO CATÁLOGO DE SERVIÇOS LOTE 01

2.1 Reconfiguração FIREWALL

2.1.1 Reinstalação de firmwares de sistemas operacionais e aplicações, bem como a reativação das licenças adquiridas no momento da primeira ativação;

2.1.2 A reinstalação dos softwares poderá contemplar as atualizações e correções fornecidas pelos fabricantes dos respectivos produtos desde que os mesmos sejam disponibilizados pelo fabricante;

2.1.3 Restauração de backup de configuração, se disponibilizado pela CONTRATANTE;

2.1.4 Reconfiguração do Firewall para que o mesmo atenda os requisitos anteriores de configuração;

2.1.5 Reconfiguração do Firewall para que o mesmo atenda os requisitos definidos pela CONTRATANTE no da emissão da Ordem de Serviço;

2.1.6 **ENTREGÁVEL**: A CONTRATADA entregará relatório de todas as atividades executadas com a devida comprovação que todos os serviços foram executados.

2.2 Serviço de capacitação técnica individual

2.2.1 Os serviços de capacitação técnica deverão contemplar a explanação teórica e prática para administradores da solução.

2.2.2 A CONTRATADA deve apresentar cronograma da capacitação técnica e caso a CONTRATANTE não concorde as datas e horários propostos pela CONTRATADA, o cronograma deverá ser planejado em comum acordo entre as partes.

2.2.3 A capacitação técnica deve ser realizada nas dependências da CONTRATANTE, com carga horária de 24 horas distribuídas em aulas de 8 horas diárias, em data e horário a ser definido entre as partes.

2.2.4 A CONTRATANTE disponibilizará sala para a capacitação técnica com infraestrutura e apoio básicos (sala com energia elétrica, ar-condicionado, cadeiras, projetor, tela de projeção, computadores).

2.2.4.1 A instalação e preparação do ambiente para realização da capacitação técnica é de responsabilidade da CONTRATANTE, e será disponibilizado pela CONTRATANTE até 72 (setenta e duas) horas antes da realização da capacitação técnica.

2.2.5 A CONTRATADA deverá fornecer manual da solução em mídia eletrônica.

2.2.6 Após o término dos serviços a CONTRATADA deverá fornecer certificados da capacitação técnica realizada.

2.2.7 Conteúdo programático:

2.2.7.1 Arquitetura de funcionamento da Solução de Segurança com subscrições;

2.2.7.2 Configuração básica para funcionamento;

2.2.7.3 Configuração de gerenciamento;

2.2.8 **ENTREGÁVEL**: A CONTRATADA disponibilizará à CONTRATANTE o relatório da execução da capacitação técnica com os seguintes dados:

2.2.8.1 Nome do participante;

2.2.8.2 Conteúdo da capacitação;

2.2.8.3 Data e Hora;

2.2.8.4 Carga horaria;

2.2.8.5 Frequência.

# APÊNDICE "C"

# PROCEDIMENTO DE AVALIAÇÃO DAS AMOSTRAS

## 1 COMISSÃO DE AVALIAÇÃO DAS AMOSTRAS

1.1 O procedimento de avaliação das amostras de que trata o item "Das Amostras" do Termo de Referência será conduzido por comissão especialmente designada pelo Ibama com a seguinte composição:

1.1.1 3 (três) integrantes do Ibama;

1.1.2 O pregoeiro responsável pelo certame.

## 2 DA ENTREGA DAS AMOSTRAS

2.1 Os softwares solicitados para análise pelo pregoeiro deverão ser entregues para a análise em até 05 (cinco) dias úteis a contar do dia subsequente a da solicitação.

2.1.1 O pregoeiro responsável pelo certame conduzirá o processo de conferências dos itens entregues, juntamente com toda a documentação fornecida pela empresa.

2.1.2 A equipe técnica da Coordenação-Geral de Infraestrutura do Ibama lavrará o termo de recebimento das amostras juntamente com o pregoeiro.

## 3 ANÁLISE DAS AMOSTRAS

3.1 Escopo de Avaliação

3.1.1 O Ibama definirá os itens e quantidades que deverão ser entregues para a amostra.

3.1.2 O Ibama definirá qual será o escopo de avaliação, incluindo avaliação dos requisitos de software e de funcionalidades. A Critério do Ibama poderá ser avaliado todos os requisitos técnicos das especificações.

3.2 Período de Avaliação

3.2.1 O processo de analise das amostras ocorrerá em até 10 (dez) dias úteis, contados do primeiro dia útil subsequente a entrega das amostras.

3.2.2 O período de avaliação poderá se estender por período superior a este mediante o despacho fundamentado do Pregoeiro, por solicitação da Comissão de Avaliação.

3.3 Local e Horário

3.3.1 As análises ocorrerão nas dependências do Ibama em local a ser definido pelo Pregoeiro na data marcada para início dos trabalhos.

## 4 FORMAS DE MENSURAÇÃO E ANÁLISE

4.1 Os técnicos da Comissão de avaliação verificarão os requisitos técnicos selecionados dentro os requisitos exigidos no Termo de Referência de forma objetiva. Para cada item avaliado será atribuído o critério **aprovado** ou **reprovado**.

4.2 Ordem da Avaliação

4.2.1 As amostras serão analisadas uma por vez, observando a ordem dos itens selecionados.

4.3 Inspeções

4.3.1 As comprovações dos requisitos poderão ser feitas da seguinte maneira:

4.3.1.1 Por verificação de software, em especial para os casos dos testes de desempenho e funcionalidades.

4.3.1.2 Por verificação de hardware, em especial para verificação de atendimento dos requisitos.

4.3.2 Avaliação dos Membros da Comissão

4.3.2.1 As anotações de aprovação e reprovação dos itens será efetuada pela comissão de avaliação em escrutínio reservado. Os membros da comissão não informarão no momento da avaliação se o item foi aprovado ou reprovado.

4.3.2.2 A reprovação de um item será sempre fundamentada e deverá constar no relatório final do processo de avaliação das amostras.

4.3.3 Regras a Serem Observadas

4.3.3.1 Durante a reunião não será permitido ao público presente o uso de telefones celulares, estes, portanto, devem permanecer desligados ou em modo reunião.

4.3.3.2 O critério observado pela a administração para atendimento a um item poderá ser visto por qualquer um dos presentes, bastando que para isso, seja solicitada a vistas.

4.3.3.3 É proibido formular questionamentos aos membros da comissão durante processo de análise, podendo estes ser feito em momento oportuno.

4.3.3.4 Os membros da administração poderão recusar ou acatá-lo parcial ou integralmente. Os questionamentos poderão ou não constar do relatório final de avaliação, a critério da Administração.

## 5 ACOMPANHAMENTO DO PROCESSO DE ANÁLISE

5.1 O processo de análise das amostras será público, obedecidas às condições aqui estabelecidas:

5.1.1 Qualquer interessado em acompanhar o processo de homologação deverá inscrever-se para o processo de avaliação das amostras enviando um e-mail para XXXXXX.@Ibama.gov.br com os seguintes dados:

5.1.1.1 Nome completo, RG, CPF e Nome da empresa.

5.1.1.2 Serão aceitas as inscrições efetivadas do momento imediatamente posterior à data de encerramento da sessão pública (de preços) até o último dia útil imediatamente anterior a data agendada para o início dos trabalhos.

5.1.1.3 Por razões de logística e acomodações necessárias a organização do processo e homologação, o número de pessoas autorizadas a acompanhar o processo de homologação será limitado a 10.

5.1.1.4 Serão selecionadas as pessoas na ordem de inscrição, limitados a 2 (duas) pessoas / representantes por empresa.

5.1.1.5 As empresas beneficiárias dos itens quanto ao preço, também deverão efetuar a inscrição de seus técnicos, ao número máximo de 3 (três).

5.1.1.5.1 O Ibama assegurará o direito de reserva de inscrições aos técnicos das empresas beneficiárias dos Itens, ainda que as inscrições sejam feitas de forma tardia.

5.1.1.6 Fica assegurado o direito dos membros da Comissão para peticionar tempo reservado para a discussão de temas relevantes, devendo todos os membros presentes ao local de avaliação retirar-se durante este período.

## APÊNDICE "D"

## DECLARAÇÃO DE VISTORIA

**DECLARO**, para fins de participação no Pregão Eletrônico SRP nº ___/____, que tomei conhecimento de todas as informações necessárias à execução de seu objeto, e que vistoriei os locais de instalação dos softwares e componentes.

Cidade/UF, _____ de_____ de ____.

_____
Carimbo e Assinatura do Responsável/Representante da Empresa
(Nome, cargo, CPF)

_____
Carimbo e Assinatura do Representante do Ibama

## APÊNDICE "E"

## DECLARAÇÃO DE RECUSA DE VISTORIA

**DECLARO**, para fins de participação no Pregão Eletrônico SRP nº ___/____, que a empresa _____, CNPJ nº _____ sito à _____ na cidade de _____ UF____, **OPTOU PELA NÃO REALIZAÇÃO DA VISTORIA TÉCNICA NAS INSTALAÇÕES FÍSICAS DO IBAMA**, tendo ciência que não poderá alegar em qualquer fase da licitação ou vigência da relação contratual que não realizará os serviços em conformidade com a qualidade e requisitos exigidos.

Cidade/UF, _____ de_____ de ____.

_____
Carimbo e Assinatura do Responsável/Representante da Empresa

**Nome legível** _____
**CPF nº.** _____

## APÊNDICE "F"

## PROPOSTA DE PREÇOS

(em papel timbrado da empresa)

**Ao**
**Instituto Brasileiro de Meio Ambiente e dos Recursos Naturais Renováveis - IBAMA**
**SCEN Trecho 2 - Edifício Sede**
**70.818-900 - Brasília, DF**

**Referência:** Pregão Eletrônico SRP nº ___/____.

Proposta que faz a empresa _____, inscrita no CNPJ nº _____ e inscrição estadual nº _____, estabelecida no(a) _____, para eventual aquisição (ou contratação) xxxxxxxx para atender às necessidades do **IBAMA**, de acordo com as especificações e condições constantes do Pregão em referência, bem como do respectivo Edital e seus Anexos.

### PLANILHA DE PROPOSTA DE PREÇOS

| ITEM | DESCRIÇÃO | UNIDADE | QTD | Valor Unitário R$ | Valor Total R$ |
|---|---|---|---|---|---|
| 1 | Solução de segurança (Firewall de Próxima Geração) com Subscrição e Produto, Incluindo instalação e transferência de conhecimento. Com 3 anos de garantia do fabricante. | UN. | 02 | | |
| | | | | TOTAL GERAL R$ | |

**1)** Dados da Proposta:

Valor Total: R$ _____ (**VALOR POR EXTENSO**).

**2)** Validade da Proposta: 60 (sessenta) dias, a contar da data de sua apresentação.

**3)** Informamos, por oportuno, que nos preços apresentados acima já estão computados todos os custos necessários decorrentes da prestação dos serviços, bem como já incluídos todos os impostos, encargos trabalhistas, previdenciários, fiscais, comerciais, taxas, seguros, deslocamentos de pessoal e quaisquer outros que incidam direta ou indiretamente.

**4)** Dados da empresa:

**a)** Razão Social: _____
**b)** CNPJ (MF) nº _____
**c)** Inscrição Estadual nº: _____
**d)** Endereço: _____

**e)** Telefone: _____ Fax: _____ e-mail: _____
**f)** Cidade: _____ Estado: _____
**g)** CEP: _____
**h)** Representante(s) legal(is) com poderes para assinar o contrato:
   a. Nome: _____
   b. Cargo: _____
   c. CPF: _____ RG: _____ _____-____
**i)** Dados Bancários:
   a. Banco:_____
   b. Agência:_____
   c. Conta Corrente:_____
**j)** Dados para Contato:
   a. Nome: _____
   b. Telefone/Ramal: _____

Declaramos, para todos os fins e efeitos legais, aceitar, irrestritamente, todas as condições e exigências estabelecidas no Edital da licitação em referência e do Contrato a ser celebrado, cuja minuta constitui o Anexo "__" do Edital.

Declaramos, ainda, que inexiste qualquer vínculo de natureza técnica, comercial, econômica, financeira ou trabalhista com serviço ou dirigente do Ibama; e que foi (realizada a Vistoria nas instalações do Ibama, tomando conhecimento dos serviços a serem realizados / apresentada recusa formal de Vistoria), não sendo admitidas, em hipótese alguma, alegações posteriores de desenvolvimento dos serviços e de dificuldades técnicas não previstas.

Local e data

_____

Representante Legal
Cargo
CPF

## APÊNDICE "G"

## ORDEM DE FORNECIMENTO (OF)

**Nº _____**

**Nome Solicitante:** **Área:**

**Ramal para contato:** **Data:** **Hora:**

**Serviço/Atividade:**

---

**Recebido por:** **Data:** **Hora:**

---

**Descrição do serviço/atividade a ser executada:**
**(o que será feito, responsabilidades, entregáveis, prazos e custo)**

---

**Responsável pela Execução do Serviço/Atividade:**

**Início:** **Data:** **Horário:**

**Término:** **Data:** **Horário:**

**Gestor IBAMA:**

---

**Situação da ordem de fornecimento:** ☐ **Executada** ☐ **Não Executada**

**Motivo:** ☐ **Infraestrutura** ☐ **Desistência de Usuário** ☐ **Outros**

**No caso de "outros" favor especificar o motivo.**

**Visto de Conclusão (Solicitante):** **Data:** **Horário:**

---

**Responsável OF**

## APÊNDICE "H"

## TERMO DE RECEBIMENTO PROVISÓRIO

| | | | |
|---|---|---|---|
| **PROCESSO ADMINISTRATIVO N.º** | | | |
| **PROCESSO LICITATÓRIO** | | | |
| **OBJETO** | | | |
| **N.º do CONTRATO** | | **N.° da OS** | |
| **CONTRATADA** | | | |
| **CNPJ** | | **Telefone**(s) | |

Por este instrumento, atestamos para fins de cumprimento do disposto no Art. 73, inciso II, alínea "a", da Lei nº 8.666, de 21 de junho de 1993, e no artigo 34, inciso I, da Instrução Normativa nº 4 do Ministério do Planejamento, Desenvolvimento e Gestão - MPOG, de 11 de setembro de 2014, que os bens e/ou serviços, relacionados no quadro abaixo, foram recebidos nesta data e serão objeto de avaliação quanto aos aspectos de qualidade, de acordo com os Critérios de Aceitação previamente definidos pelo Edital de Pregão Eletrônico SRP n° ____/____ do Ibama.

| Item | Descrição | Identificação | Unidade | Quantidade |
|---|---|---|---|---|
| | | | | |

Ressaltamos que o recebimento definitivo dos bens e/ou serviços ocorrerá em até 05 (cinco) dias, desde que não ocorram problemas técnicos ou divergências quanto às especificações constantes do instrumento contratual proveniente do Edital de Pregão Eletrônico SRP n° ____/____.

Cidade/UF, ____de _____de _____.

_____
Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

_____
Representante Legal da Empresa
Cargo
CPF

# APÊNDICE "I"

## TERMO DE RECEBIMENTO DEFINITIVO

| | | | |
|---|---|---|---|
| **PROCESSO ADMINISTRATIVO N.º** | | | |
| **PROCESSO LICITATÓRIO** | | | |
| **OBJETO** | | | |
| **N.º do CONTRATO** | | **N.° da OS** | |
| **CONTRATADA** | | | |
| **CNPJ** | | **Telefone(s)** | |

Por este instrumento, as partes abaixo identificadas atestam para fins de cumprimento do disposto no Art. 73, inciso II, alínea "b", da Lei nº 8.666, de 21 de junho de 1993, e no artigo 34, inciso VIII, da Instrução Normativa nº 4 do Ministério do Planejamento, Desenvolvimento e Gestão - MPOG, de 11 de setembro de 2014, que os bens e/ou serviços relacionados no quadro abaixo, possuem as quantidades e a qualidade compatível com as condições e exigências constantes do Edital de Pregão Eletrônico SRP n° ____/____.

| Item | Descrição | Identificação | Unidade | Quantidade |
|---|---|---|---|---|
| | | | | |

Cidade/UF, ____de _____de _____.

_____
Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

_____
Representante da Área Requisitante
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

_____
Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

_____
Representante Legal da Empresa
Cargo
CPF

## APÊNDICE "J"

## TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO

| | |
|---|---|
| PROCESSO ADMINISTRATIVO N.º | |
| PROCESSO LICITATÓRIO | |
| OBJETO | |
| CONTRATO N.º | |

**O IBAMA**, com sede em Brasília-DF, inscrito no CNPJ sob o nº _____**,** doravante denominado **CONTRATANTE** e a **Empresa** _____, estabelecida à _____, CEP: _____, inscrita no CNPJ sob o nº _____, doravante denominada simplesmente **CONTRATADA**, representada neste ato pelo **Sr** _____, (cargo) _____, (nacionalidade) _____, (estado civil) _____, (profissão) _____, portador da Cédula de Identidade nº _____, e do CPF nº _____, residente e domiciliado em _____, e, sempre que em conjunto referidas como PARTES para efeitos deste **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, doravante denominado simplesmente TERMO, e,

**CONSIDERANDO** que, em razão do atendimento à exigência do Contrato Nº ____/_____, celebrado pelas PARTES, doravante denominado **CONTRATO**, cujo objeto é a **<objeto do contrato>**, mediante condições estabelecidas pelo **IBAMA**;

**CONSIDERANDO** que o presente **TERMO** vem para regular o uso dos dados, regras de negócio, documentos, informações, sejam elas escritas ou verbais ou de qualquer outro modo apresentada, tangível ou intangível, entre outras, doravante denominadas simplesmente de **INFORMAÇÕES**, que a **CONTRATADA** tiver acesso em virtude da execução contratual;

**CONSIDERANDO** a necessidade de manter sigilo e confidencialidade, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de interesse do Ibama de que a **CONTRATADA** tomar conhecimento em razão da execução do **CONTRATO**, respeitando todos os critérios estabelecidos aplicáveis às **INFORMAÇÕES**;

O **IBAMA** estabelece o presente **TERMO** mediante as cláusulas e condições a seguir:

**CLÁUSULA PRIMEIRA - DO OBJETO**

O objeto deste **TERMO** é prover a necessária e adequada **PROTEÇÃO ÀS INFORMAÇÕES** do **IBAMA**, principalmente aquelas classificadas como **CONFIDENCIAIS**, em razão da execução do **CONTRATO** celebrado entre as PARTES.

**CLÁUSULA SEGUNDA - DAS INFORMAÇÕES CONFIDENCIAIS**

**Parágrafo Primeiro:** As estipulações e obrigações constantes do presente instrumento serão aplicadas a todas e quaisquer **INFORMAÇÕES** reveladas pelo **IBAMA**.

**Parágrafo Segundo:** A **CONTRATADA** se obriga a manter o mais absoluto sigilo e confidencialidade com relação a todas e quaisquer **INFORMAÇÕES** que venham a ser fornecidas pelo **IBAMA**, a partir da data de assinatura deste **TERMO**, devendo ser tratadas como **INFORMAÇÕES CONFIDENCIAIS**, salvo aquelas prévia e formalmente classificadas com tratamento diferenciado pelo **IBAMA**.

**Parágrafo Terceiro:** A **CONTRATADA** se obriga a não revelar, reproduzir, utilizar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que nenhum de seus diretores, empregados e/ou prepostos faça uso das **INFORMAÇÕES** do **IBAMA**.

**Parágrafo Quarto:** O **IBAMA**, com base nos princípios instituídos na Segurança da Informação, zelará para que as **INFORMAÇÕES** que receber e tiver conhecimento sejam tratadas conforme a natureza de classificação informada pela **CONTRATADA**.

**CLÁUSULA TERCEIRA - DAS LIMITAÇÕES DA CONFIDENCIALIDADE**

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

**I.** Sejam comprovadamente de domínio público no momento da revelação ou após a revelação, exceto se isso ocorrer em decorrência de ato ou omissão das PARTES;

**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 - DAS OBRIGAÇÕES ADICIONAIS**

**Parágrafo Primeiro:** A **CONTRATADA** se compromete a utilizar as **INFORMAÇÕES** reveladas exclusivamente para os propósitos da execução do **CONTRATO**.

**Parágrafo Segundo:** A **CONTRATADA** se compromete a não efetuar qualquer cópia das **INFORMAÇÕES** sem o consentimento prévio e expresso do **IBAMA**.

**I.** O consentimento mencionado no Parágrafo segundo, entretanto, será dispensado para cópias, reproduções ou duplicações para uso interno das PARTES.

**Parágrafo Terceiro:** A **CONTRATADA** se compromete a cientificar seus diretores, empregados e/ou prepostos da existência deste **TERMO** e da natureza confidencial das **INFORMAÇÕES** do **IBAMA**.

**Parágrafo Quarto:** A **CONTRATADA** deve tomar todas as medidas necessárias à proteção das **INFORMAÇÕES** do **IBAMA**, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo **IBAMA**.

**Parágrafo Quinto:** Cada PARTE permanecerá como única proprietária de todas e quaisquer **INFORMAÇÕES** eventualmente reveladas à outra parte em função da execução do **CONTRATO**.

**Parágrafo Sexto:** O presente **TERMO** não implica a concessão, pela parte reveladora à parte receptora, de nenhuma licença ou qualquer outro direito, explícito ou implícito, em relação a qualquer direito de patente, direito de edição ou qualquer outro direito relativo à propriedade intelectual.

**I.** Os produtos gerados na execução do **CONTRATO**, bem como as **INFORMAÇÕES** repassadas à **CONTRATADA**, são única e exclusiva propriedade intelectual do **IBAMA**.

**Parágrafo Sétimo:** A **CONTRATADA** firmará acordos por escrito com seus empregados e consultores ligados direta ou indiretamente ao **CONTRATO**, cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente instrumento.

**Parágrafo Oitavo:** A **CONTRATADA** obriga-se a não tomar qualquer medida com vistas a obter, para si ou para terceiros, os direitos de propriedade intelectual relativos aos produtos gerados e às **INFORMAÇÕES** que venham a ser reveladas durante a execução do **CONTRATO**.

**CLÁUSULA QUINTA - DO RETORNO DE INFORMAÇÕES**

**Parágrafo Único:** Todas as **INFORMAÇÕES** reveladas pelas PARTES permanecem como propriedade exclusiva da parte reveladora, devendo a esta retornar imediatamente assim que por ela requerido, bem como todas e quaisquer cópias eventualmente existentes.

**I.** A **CONTRATADA** deverá devolver, íntegros e integralmente, todos os documentos a ela fornecida, inclusive as cópias porventura necessárias, na data estipulada pelo **IBAMA** para entrega, ou quando não mais for necessária a manutenção das Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias.

**II.** A **CONTRATADA** deverá destruir quaisquer documentos por ela produzidos que contenham Informações Confidenciais do **IBAMA**, quando não mais for necessária a manutenção dessas Informações Confidenciais, comprometendo-se a não reter quaisquer reproduções (incluindo reproduções magnéticas), cópias ou segundas vias, sob pena de incorrer nas penalidades previstas neste Termo.

**CLÁUSULA SEXTA - DA VIGÊNCIA**

**Parágrafo Único:** O presente **TERMO** tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até 5 (cinco) anos após o término do Contrato.

**CLÁUSULA SÉTIMA - DAS PENALIDADES**

**Parágrafo Único:** 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** 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 pelo **IBAMA**, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

**CLÁUSULA OITAVA - DAS DISPOSIÇÕES GERAIS**

**Parágrafo Primeiro:** Este **TERMO** constitui vínculo indissociável ao **CONTRATO**, que é parte independente e regulatória deste instrumento.

**Parágrafo Segundo:** O presente **TERMO** constitui acordo entre as PARTES, relativamente ao tratamento de **INFORMAÇÕES**, principalmente as **CONFIDENCIAIS**, aplicando-se a todos e quaisquer acordos futuros, declarações, entendimentos e negociações escritas ou verbais, empreendidas pelas PARTES em ações feitas direta ou indiretamente.

**Parágrafo Terceiro:** Surgindo divergências quanto à interpretação do pactuado neste **TERMO** ou quanto à execução das obrigações dele decorrentes, ou constatando-se nele a existência de lacunas, solucionarão as PARTES tais divergências, de acordo com os princípios da legalidade, da eqüidade, da razoabilidade, da economicidade, da boa fé, e, as preencherão com estipulações que deverão corresponder e resguardar as **INFORMAÇÕES** do **IBAMA**.

**Parágrafo Quarto:** O disposto no presente **TERMO** prevalecerá sempre em caso de dúvida, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos legais conexos relativos à **CONFIDENCIALIDADE DE INFORMAÇÕES**.

**Parágrafo Quinto:** 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.

**CLÁUSULA NONA - DO FORO**

**Parágrafo Único:** Fica eleito o foro da Justiça Federal - Seção Judiciária do Distrito Federal, em Brasília-DF, para dirimir quaisquer dúvidas oriundas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, a **CONTRATADA** assina o presente **TERMO DE CONFIDENCIALIDADE DA INFORMAÇÃO**, em 2 (duas) vias de igual teor e um só efeito, na presença de duas testemunhas.

Cidade/UF, ___ de _____ de _____.

_____
Nome do Diretor ou representante legal da empresa
Cargo
CPF nº

_____
Gestor do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

_____
Fiscal Técnico do Contrato
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

# APÊNDICE "K"

## TERMO DE CIÊNCIA

| | | | |
|---|---|---|---|
| PROCESSO ADMINISTRATIVO N.º | | | |
| PROCESSO LICITATÓRIO | | | |
| OBJETO | | | |
| CONTRATO N.º | | CONTRATADA | |

Pelo presente instrumento, eu _____, CPF nº _____, RG nº _____, expedida em _____, órgão expedidor ____/__, prestador de serviço, ocupando o cargo de _____ na empresa _____, que firmou Contrato com o **IBAMA**, **DECLARO**, para fins de cumprimento de obrigações contratuais e sob pena das sanções administrativas, civis e penais, que tenho pleno conhecimento de minha responsabilidade no que concerne ao sigilo que deve ser mantido sobre os assuntos tratados, as atividades desenvolvidas e as ações realizadas no âmbito do Ibama, bem como sobre todas as informações que, por força de minha função ou eventualmente, venham a ser do meu conhecimento, comprometendo-me a guardar o sigilo necessário a que sou obrigado nos termos da legislação vigente.

**DECLARO**, ainda, nos termos da Política de Segurança da Informação, Informática e Comunicações do Ibama, Portaria nº 9 de 05 de Junho de 2012, estar ciente e **CONCORDO** com as condições abaixo especificadas, responsabilizando-me por:

**I.** tratar o(s) ativo(s) de informação como patrimônio do Ibama;

**II.** utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do Ibama;

**III.** não utilizar ou divulgar em parte ou na totalidade, as informações de propriedade ou custodiadas, sob qualquer forma de armazenamento, pelo Ibama sem autorização prévia do gestor ou responsável pela informação;

**IV.** contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

**V.** utilizar credenciais ou contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do Ibama;

**VI.** responder, perante o Ibama, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação.

Cidade/UF, ____de _____de _____.

_____
Nome do Funcionário
Cargo
CPF nº

Ciente:

Cidade-UF, ____de _____de _____.

_____
Nome do Diretor ou representante legal da empresa
Cargo
CPF nº

# APÊNDICE "L"

## TERMO DE ENCERRAMENTO DO CONTRATO

| | | | |
|---|---|---|---|
| PROCESSO ADMINISTRATIVO N.º | | | |
| PROCESSO LICITATÓRIO | | | |
| OBJETO | | | |
| CONTRATO N.º | | CONTRATADA | |

Por este instrumento, as partes abaixo identificadas resolvem registrar o encerramento do contrato em epígrafe e ressaltar o que segue:

O presente contrato está sendo encerrado por motivo de <motivo>.

As partes concedem-se mutuamente plena, geral, irrestrita e irrevogável quitação de todas as obrigações diretas e indiretas decorrentes do Contrato, não restando mais nada a reclamar de parte a parte, exceto as relacionadas no parágrafo a seguir.

Não estão abrangidas pela quitação ora lançada e podem ser objeto de exigência ou responsabilização, mesmo após o encerramento do vínculo contratual:

- As obrigações relacionadas a processos iniciados de penalização contratual;
- As garantias sobre bens e serviços entregues ou prestados, tanto legais quanto convencionais;
- A reclamação de qualquer tipo sobre defeitos ocultos nos produtos ou serviços entregues ou prestados;
- <inserir pendências, se houver>.

E assim tendo lido e concordado com todos os seus termos, firmam as partes o presente instrumento, em duas vias iguais, para que surta seus efeitos jurídicos.

Cidade/UF, ____ de _____ de _____.

| | |
|---|---|
| _____ | _____ |
| Gestor do Contrato | Representante da Área Requisitante |
| Matrícula | Matrícula |
| <<Cargo/Função>> | <<Cargo/Função>> |
| <<Setor/Departamento>> | <<Setor/Departamento>> |
| _____ | _____ |
| Fiscal Técnico do Contrato | Representante Legal da Empresa |
| Matrícula | Cargo |
| <<Cargo/Função>> | CPF |
| <<Setor/Departamento>> | |

# APÊNDICE "M"

## RELAÇÃO DE ENDEREÇOS E LOCALIDADES

### UNIDADE DO IBAMA - SEDE

| ITEM | UF | ENDEREÇO | CEP |
|---|---|---|---|
| 1 | DF | SCEN Trecho 2 - Ed. Sede do IBAMA - Bloco B - Sub-Solo, - Brasília | 70818-900 |

## APÊNDICE "N"

## TERMO DE EXECUÇÃO DE CAPACITAÇÃO TÉCNICA

A empresa _____, inscrita no CNPJ/MF nº _____, em atendimento ao Contrato nº _____, junto ao Ibama, por intermédio deste termo, considera finalizados a capacitação técnica da solução _____ de origem _____ desenvolvido pelo fabricante _____ na versão _____,

Os seguintes documentos acompanham este termo na comprovação da conclusão dos treinamentos:

**a)** Folha de Presença por turma – APÊNDICE Q;

**b)** Formulário de avaliação de capacitação técnica – APÊNDICE P;

Cidade/UF, _____ de _____ de ____.

_____
Representante Legal
(com carimbo da empresa)
CPF
<<Cargo/Função>>
<<CONTRATADA >>

_____
Representante do IBAMA
Matrícula
<<Cargo/Função>>
<<Setor/Departamento>>

## APÊNDICE "O"

## TERMO DE RECEBIMENTO POSIC

## DECLARAÇÃO DE RECEBIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, INFORMÁTICA E COMUNICAÇÕES DO IBAMA - POSIC

**DECLARO**, para fins de participação no Pregão Eletrônico SRP nº _____/____, que tomei conhecimento e recebi uma cópia da Política de Segurança da Informação, Informática e Comunicações do Ibama – POSIC.

Cidade/UF, _____ de_____ de ____.

_____
Carimbo e Assinatura do Responsável/Representante da Empresa
(Nome, cargo, CPF)

_____
Carimbo e Assinatura do Representante do Ibama

## APÊNDICE "P"

## FORMULÁRIO DE AVALIAÇÃO DE CAPACITAÇÃO TÉCNICA

**I – DADOS PESSOAIS:**

Nome: _____

Matrícula: _____ Ramal: _____

Lotação: _____

**II – DADOS DO EVENTO:**

Nome: _____

Empresa Promotora: _____

Local de Realização: _____

Período: _____

Instrutor(es): _____

Caro Participante,

Este questionário tem como objetivo conhecer o seu grau de satisfação em relação ao evento que acaba de participar. A sua opinião é fundamental para que possamos avaliar, dentre outros aspectos, o aproveitamento do curso e a qualidade da empresa promotora desse evento.
Solicitamos sua colaboração no sentido de responder às questões a seguir, utilizando a escala abaixo:

| | | |
|---|---|---|
| 1 | ☹ | Ruim |
| 2 | 😐 | Regular |
| 3 | ☺ | Bom |
| 4 | ☺☺ | Ótimo |
| **NA** | | Não se Aplica |

I - Quanto ao **CONTEÚDO DO EVENTO:**

| | | | | | |
|---|---|---|---|---|---|
| 1. Aquisição de novos conhecimentos | 1 | 2 | 3 | 4 | NA |
| 2. Aplicabilidade às atividades desenvolvidas | 1 | 2 | 3 | 4 | NA |
| 3. Oportunidade para atualização profissional | 1 | 2 | 3 | 4 | NA |

II - Quanto ao(s) **INSTRUTOR(ES)**:

| | | | | | |
|---|---|---|---|---|---|
| 1. Domínio do assunto | 1 | 2 | 3 | 4 | NA |
| 2. Clareza e objetividade na exposição do assunto | 1 | 2 | 3 | 4 | NA |
| 3. Capacidade de analisar e sintetizar idéias | 1 | 2 | 3 | 4 | NA |
| 4. Utilização de exemplos práticos aplicáveis a sua realidade profissional | 1 | 2 | 3 | 4 | NA |
| 5. Administração do tempo previsto | 1 | 2 | 3 | 4 | NA |
| 6. Estímulo à participação do grupo | 1 | 2 | 3 | 4 | NA |
| 7. Flexibilidade nas discussões | 1 | 2 | 3 | 4 | NA |
| 8. Presteza no atendimento às dúvidas | 1 | 2 | 3 | 4 | NA |
| 9. Clareza ao responder às perguntas | 1 | 2 | 3 | 4 | NA |

| | | | | | |
|---|---|---|---|---|---|
| 10. Organização e didática utilizada | 1 | 2 | 3 | 4 | NA |
| 11. Aproveitamento dos recursos audiovisuais disponíveis | 1 | 2 | 3 | 4 | NA |
| 12. Relacionamento com os participantes | 1 | 2 | 3 | 4 | NA |
| 13. Capacidade de administrar situações imprevistas | 1 | 2 | 3 | 4 | NA |
| 14. Ética e postura profissional | 1 | 2 | 3 | 4 | NA |
| 15. Cumprimento do conteúdo proposto | 1 | 2 | 3 | 4 | NA |

III- Quanto ao **DESEMPENHO PESSOAL**:

| | | | | | |
|---|---|---|---|---|---|
| 1. Motivação | 1 | 2 | 3 | 4 | NA |
| 2. Nível de comprometimento | 1 | 2 | 3 | 4 | NA |
| 3. Pontualidade | 1 | 2 | 3 | 4 | NA |
| 4. Satisfação quanto ao aprendizado recebido | 1 | 2 | 3 | 4 | NA |

IV- Quanto às **INSTALAÇÕES** onde ocorreu o Treinamento:

| | | | | | |
|---|---|---|---|---|---|
| 1. Condições do ambiente físico | 1 | 2 | 3 | 4 | NA |
| 2. Presteza no atendimento às solicitações dos participantes | 1 | 2 | 3 | 4 | NA |
| 3. Carga horária | 1 | 2 | 3 | 4 | NA |
| 4. Material didático (apostila, textos, etc.) | 1 | 2 | 3 | 4 | NA |
| 5. Recursos audiovisuais | 1 | 2 | 3 | 4 | NA |
| 6. Organização do Evento | 1 | 2 | 3 | 4 | NA |

## 6 COMENTÁRIOS:

**1.** Caso julgue necessário, comente sobre os itens acima: (horário, carga horária, organização, local, etc):

| |
|---|
| |
| |
| |
| |

**2.** Comente sobre a aplicabilidade dos conhecimentos adquiridos às atividades que realiza:

| |
|---|
| |
| |
| |
| |

**3.** Apresente suas sugestões, elogios e/ou críticas:

| |
|---|
| |
| |
| |
| |

## APÊNDICE "Q"

## LISTA DE PRESENÇA

Curso:
Local:
Instrutor:

Data:
Hora Início:
Hora Fim:

| Nome completo legível | Matrícula | Assinatura |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

# APÊNDICE "R"

## ESTIMATIVA DE PREÇOS

| Item | Descrição | Unidade | Quantidade | Valor Médio Unitário | Valor Médio Total |
|---|---|---|---|---|---|
| 1 | Solução de segurança (Firewall de Próxima Geração) com Subscrição e Produto, Incluindo instalação e transferência de conhecimento. Com 3 anos de garantia do fabricante. | UN | 02 | | |
| | | | | **Valor Total Estimado** | |

## APÊNDICE "S"

## MEMORIAL DE CÁLCULO

Em conformidade com o Decreto 2.271/1997, art. 2º, inciso II, e com a Instrução Normativa - STI/MP 4/2010, art. 15, inciso III, alínea 'b', apresenta-se neste apêndice o memorial de cálculo respectivo ao presente Termo de referência, como se segue.

Conforme já demonstrado em, **DA JUSTIFICATIVA**, os recursos de Tecnologias da Informação e Comunicação – TIC, estão cada vez mais alinhados a atividade finalística do Ibama. A dependência destes recursos é fato notório, cuja demanda interna por ampliação dos mesmos é constante, seja pela disponibilização de um novo acesso a rede ou pela necessidade recorrente de incremento de performance, disponibilidade e qualidade dos serviços prestados.

A demanda prevista em **Das Quantidades Demandadas**, tem sua origem e quantidades baseadas e respaldados na nova demanda que foi gerada com a necessidade de atualizar as soluções de segurança do Ibama, conforme já detalhado em **DA JUSTIFICATIVA**.

Assim posto, resta detalhado nesse apêndice o memorial de cálculo que definiu a estimativa de demanda do pretendido processo de aquisição.

| ITEM | DESCRIÇÃO | UNIDADE | QUANTIDADE | VALOR UNITÁRIO OPENNET | VALOR UNITÁRIO MORPHUS | VALOR UNITÁRIO PANORAME | VALOR MÉDIO UNITÁRIO |
|---|---|---|---|---|---|---|---|
| 1 | Solução de segurança (Firewall de Próxima Geração) com Subscrição e Produto, Incluindo instalação e transferência de conhecimento. Com 3 anos de garantia do fabricante. | UN | 2 | R$ 899.990,00 | R$ 955.300,00 | R$ 1.054.000,00 | **R$ 969.763,33** |
| | | | **TOTAL** | **R$ 1.799.980,00** | **R$ 1.910.600,00** | **R$ 2.108.000,00** | **R$ 1.939.526,67** |