

Projeto Básico COGTI 00539/2017

Consulta Pública para Aquisição de Solução de Firewall de Aplicação

1. Descrição do Objeto

1.1. Consulta pública para aquisição de Solução de *firewall* de aplicação;

2. Especificação do Objeto a ser Contratado

2.1. Características Gerais da Solução de *Firewall* de Aplicação:

2.1.1. A Solução deve ser composta de 1 (um) "Cluster de firewall de aplicação" a ser instalado na localidade do SERPRO Brasília;

2.1.2. Deve possuir ICSA (Certificado para *Web Application Firewall*) – Garantia da Efetividade na proteção a aplicações web;

2.1.3. Deve ser fornecido com todas as licenças necessárias para operacionalização da solução com no mínimo todas as funcionalidades aqui especificadas, em todos os componentes da solução, sem custo adicional para o SERPRO;

2.1.4. Deve possuir software e hardware de mesmo fabricante;

2.1.5. Deve ser instalado, em alta disponibilidade e com balanceamento de carga;

2.1.6. Deve operar, no mínimo, nos seguintes modos:

2.1.6.1. Modo ativo-ativo: onde ambos os nós permanecem ativos e com capacidade de inspeção de tráfego simultânea nos nós;

2.1.6.2. Modo ativo-passivo: onde o nó ativo inspeciona o tráfego, e o nó inativo tem capacidade de assumir automaticamente em caso de falha do principal;

2.1.7. Deve ser capaz de diferenciar, e proteger, entre *bots*, *web scraping* e usuários humanos para os ataques automatizados;

2.1.8. Deve identificar e bloquear ataques de clientes automatizados (robôs) de logins e acessos, ou seja, as tentativas de logins e acessos simultâneos em um curto intervalo de tempo entre os acessos;

2.1.9. Deve suportar as opções: *Bridge* (L2) e *Proxy* (Reverso e Transparente);

2.1.9.1. No modo *bridge*, deve ser possível configurar o recurso de tolerância à falha dos *appliances* de tal modo que, quando houver uma falha em um equipamento que o torne inoperante, seja possível o tráfego fluir através do *appliance standby* automaticamente;

2.1.10. Deve permitir modos de implementação utilizando técnicas de finalização e restabelecimento de conexões (*proxy* reverso) e análise do fluxo de dados sem interferência na conexão fim a fim (*proxy* transparente);

2.1.11. Deve ser IPv6 Ready – Garantia do suporte e conformidade da solução com o IPv6;

2.2. Arquitetura e Implantação:

2.2.1. A solução deve ser escalável em performance através de *cluster*, que deve suportar mais de dois nós;

2.2.2. Deve suportar, no mínimo, os três modos operacionais abaixo:

2.2.2.1. *Bypass* – Passagem do tráfego pelo equipamento sem atuação no fluxo de dados;

2.2.2.2. *Passive* – Detecção completa de intrusão, sem bloqueio;

2.2.2.3. *Active* – Detecção completa de intrusão, interceptação e bloqueio;

2.2.3. Deve suportar "*fail-over*" nativamente, "*fail-open*" e "*fail-close*" nas interfaces de rede, ou seja, em caso de falha do equipamento ou queda no fornecimento de energia, o tráfego não deve ser interrompido;

2.2.4. Deve suportar a especificação de um Diretório Virtual (*Virtual Directory*) no Servidor *web*, onde um grupo de filtros de segurança possam ser aplicados a cada aplicação web

(*virtual path*);

2.2.5. Deve suportar o trabalho com *Data Center* Corporativo (*Enterprise Data Center*) distribuído;

2.2.6. Deve suportar a integração com SIEM-ArcSight;

2.2.7. Capacidade de definição de escopo de inspeção por:

2.2.7.1. VLAN;

2.2.7.2. IPv4 e IPv6 nas interfaces físicas e virtuais;

2.2.7.3. URL;

2.2.7.4. Interface de rede do equipamento;

2.2.8. Suportar inspeção de tráfego criptografado, permitindo a autenticação do usuário com certificado do tipo A1 e A3 (*bypass* do certificado do usuário) do ICP Brasil;

2.2.8.1. Suportar inspeção com uso de chaves mínimas de 2048 bits;

2.3. Funcionalidades de Proteção a Aplicações:

2.3.1. A solução de *firewall* de aplicação deve proteger contra as dez principais vulnerabilidades OWASP (*Open Web Application Security Project*) em segurança de aplicações *web* (*Web Application Security*);

2.3.2. A solução de *firewall* de aplicação deve proteger, no mínimo, contra a todos os ataques classificados pelo WASC (*Web Application Security Consortium*) *Web Security Threat Classification* e outros:

2.3.2.1. *SQL injection*;

2.3.2.2. *Cross-site scripting* (XSS);

2.3.2.3. Adulteração de Parâmetros (*Parameter tampering*);

2.3.2.4. Manipulação de campos ocultos (*Hidden Field manipulation*);

2.3.2.5. Manipulação de seção/seções (*Session manipulation*);

2.3.2.6. *Cookie poisoning*;

2.3.2.7. *Stealth commanding*;

2.3.2.8. *Back-door* e opções de *debug*;

2.3.2.9. Ataques de *buffer overflow* em aplicações/aplicativos;

2.3.2.10. Ataques de força bruta;

2.3.2.11. Codificação de dados;

2.3.2.12. Navegação não autorizada;

2.3.2.13. Evasão de *gateway* (*gateway circumvention*);

2.3.2.14. Reconhecimento de *web server*;

2.3.2.15. SOAP e manipulação de serviços *web* (*web services manipulation*);

2.3.2.16. *Google hacking*;

2.3.2.17. *Anonymous proxy vulnerabilities*;

2.3.2.18. *Cookie injection*;

2.3.2.19. DoS;

2.3.2.20. Ataques tipo HTTP;

2.3.2.21. Ataques a *Web Services*;

2.3.2.22. *Zero-day malware*;

2.3.2.23. *XML External Entities*;

- 2.3.2.24. *Information Leakage*;
- 2.3.2.25. *Insufficient Authentication*;
- 2.3.2.26. *Directory Indexing*;
- 2.3.2.27. *Abuse of functionality*;
- 2.3.2.28. *Session Fixation*;
- 2.3.2.29. *OS Commanding*;
- 2.3.2.30. *Format String*;
- 2.3.2.31. *Insecure Indexing*;
- 2.3.2.32. *LDAP Injection*;
- 2.3.2.33. *Content Spoofing*;
- 2.3.2.34. *Remote File Inclusion*;
- 2.3.2.35. *Null Byte Injection*;
- 2.3.2.36. *SSL Injection*;
- 2.3.2.37. *Insufficient Session Expiration*;
- 2.3.2.38. *HTTP Response Splitting*;
- 2.3.2.39. *XPath Injection*;
- 2.3.2.40. *SYN flood*;

2.3.3. A solução de *firewall* de aplicação deve permitir aplicação de políticas em tempo real, sem a necessidade de interrupção do tráfego, independentemente da codificação de caracteres, a fim de combater a técnicas de evasão, tais como:

- 2.3.3.1. *URL-decoding* (por exemplo, %XX);
- 2.3.3.2. *Self-referencing paths* (isto é, o uso de *./* e códigos equivalentes);
- 2.3.3.3. *Path back-references* (isto é, o uso de *../* e códigos equivalentes);
- 2.3.3.4. Caracteres Maiúsculos e Minúsculos misturados;
- 2.3.3.5. Uso excessivo de espaços em branco;
- 2.3.3.6. Remoção de comentários (por exemplo, converter DELETE/**/FROM em DELETE FROM);
- 2.3.3.7. Conversão de caracteres de barra invertida, suportados pelo Microsoft Windows, em caracteres de barra normal;
- 2.3.3.8. Conversão de codificação Unicode específica IIS (%uXXYY);
- 2.3.3.9. Deve suportar formato Unicode IIS estendida;
- 2.3.4. Deve permitir forçar com que as requisições feitas (*request flows*) por um usuário através da aplicação, entre uma página *web* e outra, sejam consistentes ao comportamento esperado pela aplicação;
- 2.3.5. Deve ser capaz de operar usando modelo positivo de segurança, por meio de aprendizado ou de definição de regras que descrevem o comportamento esperado de um aplicativo ou serviço, efetuando o bloqueio de todo o tráfego que não coincide com essas regras (árvore de acesso válido);
- 2.3.6. Deve trabalhar com métodos de detecção de ataques por assinatura e por comportamento, fazendo com que, mesmo sem assinaturas atualizadas, consiga efetuar bloqueios de ataques;
- 2.3.7. Deve ter capacidade de aprendizado da estrutura da aplicação para criação dos filtros e das regras de segurança de forma automática;
- 2.3.8. Deve permitir a importação de certificados para inspeção HTTPS;

2.3.9. Deve ser capaz de receber informações de listas de endereços maliciosos e de *bot-nets*;

2.4. Tecnologias de Bloqueio:

2.4.1. Deve funcionar como um *proxy* reverso;

2.4.2. Deve ser capaz de apresentar ao usuário mensagens de erro personalizáveis quando as solicitações de aplicativos *web* são bloqueadas;

2.4.3. O sistema deve ser capaz de inspecionar e bloquear as solicitações HTTP, SOAP e XML, conforme definições abaixo:

2.4.3.1. Solicitações em não conformidade com o protocolo;

2.4.3.2. Proteção às versões HTTP 0.9, 1.0, 1.1 e 2.0;

2.4.4. Deve trabalhar com filtros de segurança:

2.4.4.1. Contra força bruta;

2.4.4.2. De proteção para banco de dados;

2.4.4.3. De proteção contra envio de arquivos, considerando tamanho, quantidade e tipo;

2.4.4.4. De proteção dos parâmetros globais dos servidores *web*;

2.4.4.5. De definição de escopo dos métodos HTTP e HTTPS permitidos e bloqueados (*HTTP methods*);

2.4.4.6. De proteção para *logging*;

2.4.4.7. De controle dos parâmetros das aplicações;

2.4.4.8. De proteção para *path-blocking*;

2.4.4.9. De controle de *safe reply*;

2.4.4.10. De proteção a sessão;

2.4.4.11. De controle de vulnerabilidades;

2.4.4.12. De controle de serviços *web*;

2.4.4.13. De proteção a XML;

2.4.4.13.1. Deve validar solicitação *post* corpo XML;

2.4.4.13.2. Deve ter capacidade de analisar os valores encapsulados em XML em parâmetros para a distribuição de filtros subsequentes de segurança para validação;

2.4.5. Deve permitir adoção de critérios de decisão para bloqueio e alerta, considerando um ou mais critérios simultâneos:

2.4.5.1. Tipo de protocolo;

2.4.5.2. Tempo e tamanho da resposta da página;

2.4.5.3. Horário;

2.4.5.4. IP de origem;

2.4.5.5. Conteúdo do *payload*;

2.4.5.6. Conteúdo do cabeçalho;

2.4.5.7. Conteúdo do *cookie*;

2.4.5.8. Código *response*;

2.4.5.9. Navegador;

2.5. Gerenciamento de Políticas:

2.5.1. Deve trabalhar com o reconhecimento de *hosts* confiáveis para que o dispositivo aprenda apenas tráfego legítimo;

2.5.2. Deve permitir que um perfil aprendido de forma automatizada possa ser ajustado

pelo administrador ou bloqueado, para que não sofra alterações;

2.5.3. Deve reconhecer alterações legítimas realizadas nas aplicações protegidas;

2.5.4. Deve suportar o controle de política granular baseada no caminho do aplicativo (*application path*);

2.5.5. Deve ter capacidade de aprender automaticamente o comportamento de uma aplicação, isto é, sem intervenção manual;

2.5.6. Deve suportar políticas de segurança *out-of-the-box*, com base no modelo de segurança negativo direcionado a uma ampla gama de ameaças de segurança;

2.5.7. Deve suportar o modelo de segurança positivo, devendo ser capaz de aprender qual perfil de tráfego é legítimo e bloquear ataques ou atividades não autorizadas;

2.5.7.1. Ao detectar um ataque ou qualquer atividade não autorizada, deve ser possível bloquear:

2.5.7.1.1. Requisições e respostas;

2.5.7.1.2. Uma conexão TCP;

2.5.7.1.3. Um determinado usuário;

2.5.7.1.4. Um específico endereço IP;

2.5.7.1.5. Um endereço IP durante um intervalo de tempo específico;

2.5.8. Deve permitir a inspeção da política que está instalada e ativa na solução de *firewall* de aplicação;

2.5.9. Deve possuir funcionalidade que ajuste dinamicamente o nível de proteção na detecção de ataques;

2.5.10. Deve possuir rastreamento de mudanças de configuração;

2.5.11. Deve suportar refinamentos automáticos nos filtros de segurança, baseados no tráfego e em estatísticas;

2.5.12. Deve possuir interface intuitiva, com a capacidade de trabalhar com políticas distintas para diferentes aplicações;

2.5.13. Deve prover funções administrativas simples e comuns, como a atualização das políticas, políticas de personalização e de relaxamento para reduzir falsos positivos;

2.5.14. Deve permitir, através de um processo simples e manual, a aceitação de falsos positivos;

2.5.15. Deve permitir a customização de políticas contra-ataques de negação de serviços (*Denial of Service*);

2.5.16. Deve suportar a configuração de *hosts* confiáveis para permitir a execução de operações não permitidas pela política adotada para uso em eventos de testes de penetração, solução de problemas (*troubleshooting*) e análise de performance;

2.5.17. Deve implementar listas brancas (*white list*) e lista negra (*black list*) para bloqueios ou liberação de acesso, sem que seja necessário realizar a consulta nos filtros e políticas de acesso;

2.5.18. A solução de *firewall* de aplicação deve suportar diferentes métodos de autenticação, tais como SSL, certificados SSL *Client*, e autenticação de cliente *proxy*;

2.5.19. Deve permitir a criação dinâmica de políticas, com aprendizado automático sobre o uso e análise do fluxo da aplicação;

2.5.20. Deve identificar e criar um perfil de utilização das aplicações, mesmo que as páginas *web* e conteúdos sejam dinâmicos, como os desenvolvidos em JavaScript, CGI, ASP, PHP e Java;

2.6. Monitoração, Logs e Relatórios:

2.6.1. Deve suportar a geração de estatísticas de desempenho da solução de *firewall* de

aplicação;

2.6.2. Deve suportar o monitoramento e desempenho do funcionamento da solução de *firewall* de aplicação;

2.6.2.1. Deve suportar o envio de alertas via syslog e SMTP;

2.6.3. Deve possibilitar o envio de eventos de auditoria para determinados servidores;

2.6.4. Deve suportar o envio de alertas para eventos suspeitos via os seguintes métodos:

2.6.4.1. Envio de e-mail;

2.6.4.2. Envio de SNMP *trap*;

2.6.4.3. Envio de syslog;

2.6.4.4. Comunicação via OPSEC ELA;

2.6.4.5. Comunicação via ODBC;

2.6.4.6. Execução de Programa ou *Script* pré-definido;

2.6.5. Sistema de Relatórios:

2.6.5.1. Deve possuir ferramenta ou módulo para geração de relatórios, possuindo, no mínimo, os seguintes tipos de relatórios:

2.6.5.1.1. Eventos por aplicações;

2.6.5.1.2. Eventos pelo filtro de segurança;

2.6.5.1.3. Eventos pela aplicação do filtro de segurança;

2.6.5.2. Deve permitir a geração de relatórios automática e manualmente;

2.6.5.3. Deve suportar a distribuição automática de relatórios por e-mail;

2.6.5.4. Deve possuir relatório com gráfico que demonstre a distribuição de violações de segurança que ocorrem em cada aplicação *web* em relação a totalidade das aplicações *web*;

2.6.5.4.1. O relatório deve mostrar o nome da aplicação *web*, o número de eventos, e a taxa percentual de todos os eventos por aplicação;

2.6.5.5. Deve possuir relatório onde mostre a distribuição de falhas de segurança capturadas para cada filtro e regra de segurança, exibindo o nome do filtro e da regra, o número de eventos e a taxa percentual de todos os eventos por filtro e regra;

2.6.5.6. A geração de relatórios deve ser feita em todos modos de implementação de monitoramento ou *proxy*;

2.6.5.7. Deve permitir emissão de relatório com gráficos indicando tipo de ataque, violação, URL, IPs de origem e destino e localização geográfica do IP;

2.6.5.8. Deve ser possível exportar os relatórios gerados para arquivos nos formatos HTML, PDF, XML e CSV;

2.7. Interface de Gerência:

2.7.1. A Solução de *firewall* de aplicação deve ser fornecida com uma central unificada para gerenciamento e controle com interface gráfica (GUI);

2.7.1.1. A interface gráfica (GUI) de gerenciamento deve ser *cross-platform*, preferencialmente em *web* via protocolo HTTPS, com suporte a acesso nativo via Microsoft Windows, Linux, FreeBSD e Mac-OS;

2.7.1.2. Para interface gráfica do tipo *web*, deve suportar no mínimo o navegador Mozilla Firefox ESR mais recente.

2.7.2. A Solução deve possuir uma única console de segurança que permita a organização, gerenciamento e aplicação das políticas de segurança em todos os equipamentos participantes de um sistema de clusters;

2.7.3. A gerência deve se comunicar com os itens gerenciados (*appliances*) e

gerenciadores (clientes de administração) através de protocolos criptografados;

2.7.4. A Gerência deve ter capacidade de analisar eventos em tempo real e opção de geração relatórios durante a avaliação do tráfego;

2.7.5. Deve possuir *dashboard* com gráficos estatísticos por servidores e visão gráfica da estrutura da aplicação;

2.7.6. A solução de gerenciamento deve fornecer as seguintes funcionalidades no seu ambiente gráfico:

2.7.6.1. Gerenciar centralmente múltiplos *web application firewalls* espalhados pela corporação;

2.7.6.2. Configurar e executar os refinamentos das políticas de segurança através de interface intuitiva, sem a necessidade de escrever regras;

2.7.6.3. Atribuir políticas de segurança para segmentos configuráveis e altamente granulares da camada de aplicação *web*;

2.7.7. Obter e analisar eventos em tempo real e relatórios gerados durante a avaliação do tráfego;

2.7.7.1. Permitir utilizar as informações obtidas para refinar as políticas de segurança atuais;

2.7.7.2. Permitir a possibilidade de ativar o recurso de configuração automática, que reúne tráfego e dados estatísticos, a fim de determinar refinamentos automáticos para filtros de segurança;

2.7.8. Administrar o provisionamento de usuários, a distribuição de eventos e outros componentes e serviços;

2.7.9. Deve suportar o gerenciamento remoto, seguro, baseado em perfis de administração com granularidade de funções;

2.7.10. Deve permitir a criação no mínimo, dos seguintes perfis:

2.7.10.1. Administradores – Direitos administrativos completos;

2.7.10.1.1. Permitir a adição e remoção usuários;

2.7.10.1.2. Permitir mudança de permissões e senhas;

2.7.10.1.3. Visualizadores – Ver a configuração da solução e mudar a própria senha;

2.7.10.2. Dono de aplicação – Fazer alterações somente para aplicações *web* atribuídas;

2.7.10.3. Visualizador e dono de aplicação – Fazer alterações somente para os aplicativos da *web* atribuídos, e visualizar as propriedades de todos os objetos usados na solução;

2.7.10.4. Visualizador de aplicação – Visualizar a aplicação *web* atribuída ao usuário;

2.7.11. Deve permitir a exportação e importação de regras e políticas para um novo dispositivo de forma simples;

2.7.12. Deve permitir gestão e controle simplificados e centralizados para a sincronização de configuração e o compartilhamento dos dados aprendidos para todos os dispositivos;

2.7.13. Deve suportar integração com sistemas de gerenciamento corporativo de terceiros;

2.7.14. Deve suportar a recuperação do sistema via USB;

2.7.15. Deve permitir o armazenamento de sua configuração em memória não volátil, no caso de uma queda e posterior restabelecimento da alimentação, voltar à operação normalmente na mesma configuração anterior à queda de alimentação;

2.7.16. A solução de *firewall* de aplicação deve continuar analisando e tratando o tráfego corrente sem interrupção, caso os *appliances* percam a comunicação com servidores de gerência, local ou centralizada;

2.8. Demais características do Appliance:

2.8.1. Deve possuir hardware dedicado para inspeção otimizada de tráfego criptografado

com SSL e TLS;

2.8.2. A latência inserida no tráfego SSL não pode superar os 5 ms (cinco milissegundos);

2.8.3. Deve no mínimo ter capacidade 70.000 (setenta mil) conexões web concorrentes;

2.8.4. Deve suportar no mínimo 5Gbps (cinco Gigabits por segundo) de tráfego não criptografado e 2Gbps de tráfego criptografado, inspecionados simultaneamente em cada nó;

2.8.5. Interfaces para a Inspeção do Tráfego:

2.8.5.1. Deve ser fornecido com no mínimo 2 (duas) portas 10 Gigabit Ethernet Fibra;

2.8.5.2. Deve ser fornecido com no mínimo 4 (quatro) portas Gigabit Ethernet Fibra;

2.8.6. Para o gerenciamento dos Appliances:

2.8.6.1. Deve ser fornecido com no mínimo 2 (duas) portas Gigabit Ethernet Cobre (UTP), específicas para Gerenciamento;

2.8.7. Deve possuir dispositivos luminosos que indiquem estado e atividade das interfaces de rede;

2.8.8. Deve ser fornecido com no mínimo 2 (duas) portas USB;

2.8.9. Deve ter suporte ao protocolo de monitoração SNMP v1, SNMP v2c e SNMP v3;

2.8.10. Deve ser fornecido com capacidade de armazenamento de no mínimo 6TB (seis Terabytes) em cada nó do cluster com capacidade de tolerância à falha RAID 5 ou equivalente superior;

2.8.11. Deve ser fornecido com fontes de alimentação hot swappable e suportar tensão alternada entre 100-240V (cem até duzentos e quarenta volts);

2.8.12. RoHS – Os equipamentos devem seguir o padrão de controle de emissão e utilização de produtos químicos;

3. Níveis de Serviço

3.1. Garantia, Suporte e Atualização de versão de software.

3.1.1. A garantia da solução, bem como da atualização dos softwares e *patches* será de 36 (trinta e seis) meses, a partir do recebimento definitivo do SERPRO;

3.1.2. A garantia engloba sanar dúvidas relacionadas com a instalação, configuração e softwares contratados;

3.1.3. A atualização deverá englobar:

3.1.3.1. Fornecimento de versão, *release* ou *patches* mais recentes;

3.1.3.2. Fornecimento de versão mais recente da base de conhecimento;

3.1.3.3. O serviço de atualização deve incluir correções na solução ou execução de quaisquer medidas necessárias para sanar falhas de funcionamento ou vulnerabilidades da solução;

3.1.4. A cada nova versão instalada, a CONTRATADA deverá apresentar as novas funcionalidades de acordo com a solicitação do SERPRO, sem ônus adicional;

3.1.5. A garantia de 36 (trinta e seis) meses contemplará atendimento técnico quanto à configuração e solução de problemas envolvendo o produto ofertado, bem como a atualização dos softwares;

3.1.6. Caso a solução fornecida seja descontinuada na linha de comercialização do fabricante, durante a vigência da garantia, a CONTRATADA deverá manter as condições da garantia nesta contratação explicitada, ou providenciar a substituição por outra solução disponível que executem as mesmas funcionalidades exigidas no edital, sem ônus adicionais para o SERPRO;

3.1.7. Para Solução ofertada, a CONTRATADA deverá realizar, no exercício da garantia, intervenções preventivas, sendo de responsabilidade da CONTRATADA prover todas as

correções e atualizações necessárias, de forma sistemática e programada, de acordo com a periodicidade e os procedimentos especificados na documentação do fabricante;

3.1.8. A CONTRATADA deve entregar um cronograma de manutenção preventiva para aprovação do SERPRO;

3.1.9. A CONTRATADA deverá entregar, a cada intervenção preventiva realizada, relatório técnico contendo os procedimentos executados;

3.1.10. Nas intervenções preventivas ou corretivas, em que haja risco de indisponibilidade total ou parcial, o SERPRO deverá ser previamente notificado para que se proceda a aprovação e o agendamento da operação em horário conveniente ao SERPRO;

3.2. Dos Níveis de Serviço e sancionamentos

3.2.1. O exercício da garantia para retorno de hardware e software à condição operacional da solução deverá ser realizado conforme critérios abaixo:

3.2.1.1. O atendimento deve ser prestado 10 (dez) horas por dia, das 8 às 18 horas, de segunda-feira a sexta-feira, excluindo os feriados, exceto para os chamados de atividades programadas;

3.2.1.2. O atendimento aos chamados para o exercício da garantia deverá obedecer à seguinte classificação quanto ao nível de severidade:

Tabela dos Níveis de Serviço e sancionamentos						
Severidade	Descrição	Tipo	Tempo de Atendimento	Tempo de Solução	Observações	Penalidades
1-Altamente Crítica	Chamados referentes a situações de emergência ou problema crítico, caracterizados pela existência de ambiente paralisado.	On-site	No máximo 4 (quatro) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 6 (seis) horas após a abertura do chamado para resolução ou aplicação de solução de contorno	Os chamados classificados com Severidade 1 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, excluindo feriados, horário local.	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,2% (zero vírgula dois por cento) do valor contratual, por hora ou fração de hora de atraso.
2 – Crítica	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho.	On-site	No máximo 4 (quatro) horas após a abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 8 (oito) horas após a abertura do chamado.	Os chamados classificados com Severidade 2 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, excluindo feriados, horário local.	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,15% (zero vírgula quinze por cento) do valor contratual, por hora ou fração de hora de atraso.
3 – Alta	Chamados referentes a situações de baixo impacto ou problemas que se apresentem de forma intermitente, incluindo casos em que haja necessidade de substituição de	Remoto, com exceção das situações em que seja necessária intervenção física.	No máximo 6 (seis) horas após a abertura do chamado.	No máximo 10 (dez) horas após a abertura do chamado.	Os chamados classificados com Severidade 3 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, excluindo feriados, horário local.	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,1% (zero vírgula um por cento) do valor contratual, por hora ou fração de hora de atraso.

Tabela dos Níveis de Serviço e sancionamentos						
Severidade	Descrição	Tipo	Tempo de Atendimento	Tempo de Solução	Observações	Penalidades
	componentes que possuam redundância.					
4 – Média	Chamados com objetivo de solicitar acompanhamento técnico presencial para o desligamento e posterior ligação de equipamentos em virtude de atividade programada.	On-site	No máximo 24 (vinte e quatro) horas após a abertura do chamado.	Conforme agendamento.	O atendimento deverá ser realizado conforme o agendamento, mesmo que contemple períodos noturnos e dias não úteis.	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,075% (zero vírgula zero setenta e cinco por cento décimos por cento) do valor contratual, por hora ou fração de hora de atraso.
5 – Baixa	Chamados com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto.	Remoto	No máximo 24 (vinte e quatro) horas após a abertura do chamado.	No máximo 72 (setenta e duas) horas após a abertura do chamado.	Os chamados classificados com Severidade 5 serão atendidos em horário comercial, ou seja, das 08:00 às 18:00, de segunda-feira a sexta-feira, excluindo feriados, horário local.	O não atendimento dentro do prazo estabelecido para o chamado, ensejará em aplicação de multa à CONTRATADA no valor de 0,05% (zero vírgula zero cinco por cento) do valor contratual, por hora ou fração de hora de atraso.

3.2.2. Será aberto um chamado técnico para cada problema reportado, sendo iniciada a contagem do tempo de atendimento a partir da hora de acionamento;

3.2.3. Durante o período de garantia, a CONTRATADA deverá fornecer informações sobre as correções a serem aplicadas ou a própria correção;

3.2.4. Deve fornecer orientações para diagnóstico de problemas e ajuda na interpretação de traces, *dumps* e *logs*;

3.2.5. Nos casos de problemas não documentados, os registros enviados pelo SERPRO (tais como: *traces*, *dumps* e *logs*) devem ser encaminhadas aos laboratórios do responsável técnico, a fim de que sejam fornecidas as devidas correções;

3.3. Canais de Atendimento e Entrega de Relatórios

3.3.1. Atendimento por meio de canal telefônico gratuito 0800 ou tarifação reversa, e site na internet para abertura de chamado;

3.3.2. Mensalmente deverá ser entregue relatório constando os acionamentos técnicos abertos, em andamento e encerrados no período do exercício da garantia, por regional do SERPRO;

3.3.3. O relatório deve conter no mínimo as seguintes informações: número de acionamento, descrição da ocorrência, severidade, nome do responsável do SERPRO pela abertura do chamado, data e hora de abertura do chamado, data e hora do início do atendimento, tipo do atendimento (remoto ou on-site), data e hora de encerramento ou aplicação de solução de contorno e descrição da resolução adotada;

3.3.4. O relatório deverá ser entregue mesmo quando não houver chamados no período;

4. Forma de Pagamento

4.1. O pagamento será efetuado no primeiro dia útil após o 20º (vigésimo) dia corrido da data do aceite do recebimento definitivo dos equipamentos/licenças, referente a Nota Fiscal e/ou Fatura entregue no Protocolo Geral do SERPRO ou através do endereço eletrônico a ser informado pelo Gestor do Contrato;

4.1.1. O prazo para o aceite, por parte do SERPRO, será de 10 (dez) dias úteis, a partir da data de conclusão de cada entrega;

4.2. Constatando alguma incorreção nas Notas Fiscais e/ou Faturas que desaconselhe o seu pagamento, o prazo será contado a partir da respectiva regularização. O uso da carta de correção será admitida nos casos previstos pelas legislações tributárias;

4.3. A Nota Fiscal e/ou Fatura deverá ser emitida para o Serviço Federal de Processamento de Dados (SERPRO), conforme endereço e CNPJ do (s) local (is) de entrega;

4.4. A contratada deverá informar o CNPJ que será utilizado na emissão das notas fiscais e faturas;

5. Seleção do fornecedor

5.1. Em atendimento ao estabelecido no Decreto 5.450/2005, por se tratar de serviço comum, assim entendido por decorrência dos padrões de desempenho e qualidade estarem objetivamente definidos por meio de especificações usuais do mercado, a aquisição deverá ser na Modalidade de Pregão, na forma Eletrônica e adjudicação pelo menor valor global;

5.2. Avaliação de Amostra:

5.2.1. Ao licitante classificado em primeiro lugar, o SERPRO exigirá avaliação de amostra, que consiste na comprovação das funcionalidades descritas nas Especificações do objeto deste Edital;

5.2.2. Após o aceite da documentação comprobatória, a LICITANTE vencedora deverá disponibilizar todos os recursos necessários para a realização de avaliação de amostra;

5.2.3. A entrega dos equipamentos e licenças necessárias à avaliação de amostra deverá ocorrer em até 10 (dez) dias corridos contados a partir da solicitação formal do SERPRO;

5.2.4. O prazo de execução da avaliação de amostra será de 20 (vinte) dias corridos a contar da entrega;

5.2.4.1. O prazo de avaliação de amostra poderá ser prorrogado a critério do SERPRO;

5.2.5. A aceitação final da proposta da LICITANTE VENCEDORA somente será realizada após a aprovação em testes de bancada, na avaliação de amostra, descritas nesta seção;

5.2.6. Esta etapa caberá à LICITANTE VENCEDORA, para todos os itens e subitens especificados para a avaliação de amostra, comprovar na prática, por meio dos testes de bancada, nas etapas da avaliação de amostra, das características e funcionalidades exigidas;

5.2.7. Esta etapa será executada por prepostos do SERPRO em conjunto com os prepostos das LICITANTES no ITEM específico da aquisição;

5.2.8. Os testes de bancada, nas etapas da avaliação de amostra, serão realizados nas dependências do SERPRO, endereço descrito no subitem a seguir:

5.2.8.1. REGIONAL BRASÍLIA/DF, SGAN Av. L2 Norte Quadra 601 – Módulo G – Brasília/Distrito Federal, CEP: 70830-900, Telefone Geral: 0XX(61) 2021-9000, Fax: 0XX(61) 2021-9806, INSCRIÇÃO ESTADUAL: 07334743/002-94, INSCRIÇÃO MUNICIPAL: 07334743/002-94 e CNPJ: 33.683.111/0002-80;

5.2.9. Todos os testes de bancada, nas etapas da avaliação de amostra, e relacionamento dos técnicos da LICITANTE com o SERPRO deverão ser efetuados no idioma português;

5.2.10. Ao fim de cada dia de testes de bancada, nas etapas da avaliação de amostra, deverá ser emitida, assinada e distribuída Ata de Atividades e Ocorrências a todos os presentes;

5.2.11. Se um subitem referente às especificações for considerado não atendido, não

sendo corrigidos nos prazos estabelecidos, a proposta, em avaliação de amostra, será totalmente desclassificada;

5.2.12. Cada LICITANTE poderá indicar previamente os nomes de, no máximo, 02 (dois) técnicos nas etapas da avaliação de amostra. Esses técnicos deverão ser representantes legais da LICITANTE, comprovado por meio de documentação de vínculo contratual ou procuração;

5.2.12.1. Entre os técnicos indicados apenas 1 (um) técnico poderá acompanhar os testes de avaliação de amostra;

5.2.13. A critério da LICITANTE VENCEDORA, as etapas da avaliação de amostra poderão ser executadas com apoio de no máximo um técnico do fabricante;

5.2.14. As indicações deverão ser realizadas com, no mínimo, 2 (dois) dias úteis de antecedência e apenas serão permitidos questionamentos diretos aos técnicos do SERPRO;

5.2.15. No caso de ausência, em qualquer dos períodos durante a realização dos testes de bancada, nas etapas da avaliação de amostra, dos técnicos indicados pelas demais empresas concorrentes do pregão, não serão aceitos quaisquer questionamentos sobre sua realização;

5.2.16. Durante a realização dos testes de bancada, nas etapas da avaliação de amostra, serão permitidas somente 02 (duas) atualizações de software e sistema operacional da solução sob avaliação, visando a correção ou adaptação para atendimento aos requisitos do edital. Essas atualizações poderão corrigir mais de um item simultaneamente;

5.2.17. A critério do SERPRO os testes de bancada, nas etapas da avaliação de amostra, poderão ser reiniciados após atualização de versão;

5.2.18. Os testes deverão ser realizados no horário compreendido entre 09:00 e 17:00 de segunda-feira a sexta-feira;

5.2.19. A avaliação de amostra da solução ofertada deverá ser instalada sem nenhum custo para o SERPRO;

5.2.20. A licitante que for reprovada na avaliação de amostra não terá direito a qualquer indenização;

5.2.21. Será emitido um relatório descrevendo os exames realizados e contendo a aprovação ou não da avaliação de amostra;

5.2.22. Somente após todos testes de bancada, nas etapas da avaliação de amostra, será emitindo o parecer técnico aprovando ou não a amostra apresentada.

5.2.23. Os equipamentos utilizados na fase de amostra poderão ser utilizados na instalação da entrega da solução, desde que sejam novos e sem uso;

5.2.24. A documentação, bem como os manuais necessários para a homologação, deverão estar disponíveis para os representantes do SERPRO;

6. Gerenciamento contratual

6.1. Obrigações da Contratada:

6.1.1. Promover a instalação e configuração da solução, incluindo todos equipamentos previstos no projeto, nos ambientes do SERPRO, deixando-os em perfeitas condições de uso;

6.1.2. Responsabilizar-se por toda e qualquer despesa, independente da sua natureza, decorrente das instalações supramencionadas;

6.1.3. São de responsabilidade da contratada os seguintes itens: frete, seguro, embalagens, manuais, despesa de transporte ou quaisquer custos relacionados a entrega, instalação e repasse de conhecimento;

6.2. Repasse De Conhecimento

6.2.1. A CONTRATADA deve prover o repasse de conhecimento dos profissionais do

SERPRO para configuração e operação da solução;

6.2.2. A CONTRATADA deve repassar o conhecimento sem ônus adicional para o SERPRO, incluindo todo o material didático necessário;

6.2.3. O material de aula deverá abordar conteúdo teórico e prático, e deverá ser submetido ao SERPRO para aprovação antes da realização da capacitação;

6.2.4. Após a assinatura do contrato, a CONTRATADA deverá realizar o repasse do conhecimento da solução, que poderá ocorrer em paralelo a fase de instalação;

6.2.5. A CONTRATADA deve repassar o conhecimento através de profissionais habilitados e credenciados pelos fabricantes ou empresa credenciada para tal finalidade;

6.2.6. Deve ser entregues pela CONTRATADA antes do início do repasse de conhecimento todo o material didático;

6.2.7. A CONTRATADA deverá providenciar a capacitação para 2 (duas) turmas em Brasília, com capacidade para 8 (oito) participantes cada, abordando toda solução ofertada envolvendo teoria e prática, em datas a serem negociadas entre o SERPRO e a CONTRATADA;

6.2.7.1. A carga horária mínima para cada turma deverá ser de 40 (quarenta) horas;

6.2.7.2. A CONTRATADA deverá disponibilizar toda infraestrutura necessária ao repasse de conhecimento em local externo de responsabilidade da CONTRATADA (sendo aceita máquinas virtuais, desde que na mesma versão do software fornecida ao SERPRO);

6.2.8. O repasse de conhecimento deve abordar os módulos: operação básica e avançada da solução de auditoria de *firewall*, customização e gestão de fluxos, com conteúdo teórico e prático com seguinte conteúdo mínimo:

6.2.8.1. Instruções de instalação, incluindo resolução de problemas;

6.2.8.2. Instruções de manuseio e operação, incluindo resolução de problemas;

6.2.8.3. Devem ser fornecidas as instruções de utilização também em formato de videoconferência;

6.2.9. A CONTRATADA deverá apresentar uma ementa do repasse que será aprovada pelo SERPRO;

6.2.10. O repasse de conhecimento será avaliado pelos participantes do SERPRO e caso não será atingido a média de 70% pela avaliação das turmas, o repasse deverá ser revisto e realizado novamente;