

Projeto Básico COGTI 0845/2012

Consulta Pública para aquisição de solução de análise de segurança em aplicações web

1.0 Objeto

Consulta Pública para aquisição de solução de análise de segurança em aplicações web para realizar testes de segurança na metodologia caixa-preta.

2.0 Especificação do Objeto a ser Contratado

O software de análise de segurança em aplicações web deverá conter as seguintes funcionalidades:

2.1. Suporte a protocolos

A solução de análise de segurança em aplicações Web deverá suportar os seguintes protocolos:

- 2.1.1. HTTP 1.1;
- 2.1.2. HTTP 1.0;
- 2.1.3. SSL/TLS;
- 2.1.4 . HTTP Keep-Alive;
- 2.1.5 . HTTP Compression;
- 2.1.6 . Configuração de HTTP User Agent string.

2.2. Autenticação

A solução de análise de segurança em aplicações Web deverá suportar os seguintes métodos de autenticação:

- 2.2.1. Básica;
- 2.2.2. Digest;
- 2.2.3. HTTP Negotiate (NTLM e Kerberos);
- 2.2.4. HTML baseado em formulários:
 - 2.2.4.1. Automatizado;
 - 2.2.4.2. Scripted;
 - 2.2.4.3. Não-automatizado;
 - 2.2.4.5. Single Sign On;
- 2.1.5. Certificados de Cliente SSL;
- 2.1.6. Implementações customizadas

2.3. Gestão de Sessão

2.3.1. Capacidades da Gestão de Sessão

A solução deverá suportar os seguintes critérios:

- 2.3.1.1. Compreender que a aplicação está solicitando o início de uma nova sessão, usando um determinado tipo de token, como único método de identificação desta sessão;
- 2.3.1.2. Realizar uma atualização de token de sessão, quando instruída a fazê-la pela aplicação;
- 2.3.1.3. Detectar que uma sessão realizada atualmente, foi invalidada pelo aplicativo (sessão expirada);
- 2.3.1.4. Iniciar uma nova sessão e requisitar novos tokens em caso de expiração.

2.3.2. Suporte ao tipo de Token da Gestão de Sessão

A solução de análise de segurança em aplicações Web deverá suportar os seguintes tipos de tokens de gerenciamento de sessão:

- 2.3.2.1. Cookies HTTP (RFC 2965);
- 2.3.2.2. Parâmetros de HTTP;
- 2.3.2.3. Caminho da URL HTTP.

2.3.3. Configuração de Detecção de Token de Sessão

A solução de análise de segurança em aplicações Web deverá permitir a customização das seguintes configurações de token de sessão:

- 2.3.3.1. Detecção Automática de Token de Sessão e Atualização de Valor: Detectar tokens de sessão e decidir quais tokens devem ser automaticamente rastreados ou atualizados durante a

verificação;

2.3.3.2. Configuração Manual de Token de Sessão: Permitir que o usuário defina o que identifica um token de sessão, baseado em parâmetros HTTP, cookies ou qualquer outro tipo de configuração relevante.

2.3.4. Política de Atualização de Token de Sessão

2.3.4.1. A configuração de sessão da solução deverá permitir ao usuário definir quando, ou qual fase da varredura, os tokens de sessão serão atualizados. As seguintes opções de configuração deverão ser fornecidas:

2.3.4.1.1. Valor Fixo de Token de Sessão: Quando um token de sessão está configurado para usar um valor fixo, esse valor nunca mudará durante a varredura;

2.3.4.1.2. Valor de Token fornecido durante processo de Login: Quando a solução de análise de segurança logar na aplicação deverá permitir extrair valores de token que foram emitidos como parte do processo de login, até a constatação que a sessão foi invalidada;

2.3.4.1.3. Valor de Token Dinâmico: A solução utilizará sempre o valor mais recente da sessão de token, fornecida pela aplicação. Durante a fase de rastreamento ou teste de varredura, caso um novo valor seja detectado, a solução deverá atualizar todos pedidos HTTP subsequentes com o valor mais recente.

2.4. Rastreamento (Crawling)

2.4.1. Configuração de Web Crawler

Com relação ao rastreamento, a solução de análise de segurança em aplicações Web deverá:

2.4.1.1. Fornecer ao usuário a opção de definir uma URL inicial;

2.4.1.2. Fornecer ao usuário a opção de definir nomes de host adicionais (ou endereços IP) em uma lista ou um intervalo;

2.4.1.3. Fornecer ao usuário a opção de definir exclusões para:

2.4.1.3.1. Hostnames específicos (ou endereços IP);

2.4.1.3.2. URLs específicas ou padrões de URLs (expressões regulares);

2.4.1.3.3. Extensões específicas de arquivos;

2.4.1.3.4. Parâmetros específicos;

2.4.1.4. Fornecer ao usuário a capacidade de otimizar (tuning) o rastreador. Todavia, deverá permitir a limitação de requisições redundantes;

2.4.1.5. Fornecer ao usuário a opção de suportar sessões simultâneas;

2.4.1.6. Fornecer ao usuário a opção de configurar a quantidade de subníveis utilizados para a navegação, em uma estrutura Web, a partir da página inicial.

2.4.2. Funcionalidade do Web Crawler

Durante a operação, a solução deverá:

2.4.2.1. Identificar os hostnames recém-descobertos;

2.4.2.2. Suportar o envio de formulário automatizado;

2.4.2.3. Detectar páginas de erro e respostas 404 personalizadas;

2.4.2.4. Suportar Redirecionamento:

2.4.2.4.1. Seguir redirecionamentos HTTP;

2.4.2.4.2. Seguir redirecionamentos Meta Refresh;

2.4.2.4.3. Seguir redirecionamentos JavaScript;

2.4.2.5. Identificar e aceitar cookies: Reconhecer estes cookies, armazená-los e enviá-los de volta ao servidor web enquanto realiza o processo;

2.4.2.6. Suportar aplicações AJAX: Submeter automaticamente requisições XmlHTTP que são encontradas durante o processo de rastreamento.

2.5. Análise (Parsing)

2.5.1. Tipos de Conteúdo Web

A solução deverá ser capaz de analisar os seguintes tipos de conteúdo para extrair informações sobre a estrutura e funcionalidade da aplicação:

2.5.1.1. HTML;

2.5.1.2. JavaScript;

2.5.1.3. VBScript;

- 2.5.1.4. Plaintext;
- 2.5.1.5. Flash/RIA (Rich Internet Applications);
- 2.5.1.6. Protocolo AMF (Action Message Format);
- 2.5.1.7. CSS (Cascading Style Sheets);
- 2.5.1.8. Web 2.0 applications.

2.5.2. Suporte a Web Services

2.5.2.1. A solução deverá ser capaz de suportar a análise de segurança em arquiteturas orientadas a serviço e webservices, incluindo:

- 2.5.2.1. XML;
- 2.5.2.2. WSDL.

2.5.3. Suporte a Character Encoding

2.5.3.1. A solução de análise de segurança em aplicações Web deverá ser capaz de analisar e compreender o conteúdo codificado nos seguintes tipos de codificação:

- 2.5.3.1.1. ISO-8859-1;
- 2.5.3.1.2. UTF-7;
- 2.5.3.1.3. UTF-8;
- 2.5.3.1.4. UTF-16.

2.5.4. Tolerância

2.5.4.1. Os analisadores de conteúdo deverão ser capazes de lidar com conteúdos parciais ou mal formados e, ainda, capazes de extrair as informações relevantes a partir das respostas da aplicação;

2.5.5. Customização

2.5.5.1. A solução de análise de segurança em aplicações Web deverá permitir a customização do usuário para a extração de link e conteúdo;

2.5.6. Extração de Conteúdo Dinâmico (Execução Lógica de Client-Side)

2.5.6.1. A solução de análise de segurança em aplicações Web deverá ser capaz de emular a interação do usuário com a lógica do lado do cliente, com finalidade de extrair informações de forma dinâmica;

2.6. Testes

2.6.1. Teste de configuração

A solução deverá fornecer a capacidade de configurar e implementar filtros com base nos seguintes critérios:

- 2.6.1.1. Nomes de Host ou endereços IP;
- 2.6.1.2. Padrões de URLs;
- 2.6.1.3. Extensões de arquivos;
- 2.6.1.4. Parâmetros;
- 2.6.1.5. Cookies;
- 2.6.1.6. Cabeçalhos HTTP.

2.6.2. Capacidades de Teste

A solução de análise de segurança em aplicações Web deverá testar as seguintes vulnerabilidades e fragilidades de arquitetura:

2.6.2.1. Autenticação:

- 2.6.2.1.1. Força Bruta;
 - 2.6.2.1.1.1. Ausência de bloqueio de logons sucessivos;
 - 2.6.2.1.1.2. Mensagem de falha de login diferenciada para login e senhas válidas e inválidas ;
- 2.6.2.1.2. Autenticação Insuficiente;
- 2.6.2.1.3. Logon por Força Bruta;
- 2.6.2.1.4. Falta de SSL em páginas de login;
- 2.6.2.1.5. Recurso de Auto-completar não desabilitado em parâmetros de senha.

2.6.2.2. Autorização:

- 2.6.2.2.1. Previsão de Credencial/Sessão:
 - 2.6.2.2.1.1. Token de Sessão Sequencial;
 - 2.6.2.2.1.2. Token de Sessão Não-Aleatória.
- 2.6.2.2.2. Autorização Insuficiente:

- 2.6.2.2.2.1. Habilidade para forçar a navegação por URLs que exigem Login sem estar "logado";
- 2.6.2.2.2.2. Habilidade para forçar a navegação por URLs com alto privilégio, enquanto "logado" com uma conta de baixo privilégio;
- 2.6.2.2.2.3. Adulteração de método HTTP;
- 2.6.2.2.2.3. Expiração de sessão Insuficiente;
- 2.6.2.2.4. Fixação de sessão:
 - 2.6.2.2.4.1. Incapacidade de gerar ID de nova sessão após login;
 - 2.6.2.2.4.2. Gerenciamento de sessão permissiva;
- 2.6.2.2.5. Fraquezas de Sessão:
 - 2.6.2.2.5.1. Token de sessão passado em URL;
 - 2.6.2.2.5.2. Cookie de sessão não configurado com atributo de segurança;
 - 2.6.2.2.5.3. Cookie de sessão não configurado com atributo HTTPOnly;
 - 2.6.2.2.5.4. Cookie de sessão com identificador não suficientemente randômico;
 - 2.6.2.2.5.5. Site não força conexão SSL;
 - 2.6.2.2.5.6. Site usa SSL , mas referencia objetos inseguros;
 - 2.6.2.2.5.7. Site suporta cifras SSL fracas;
- 2.6.2.3. Ataques do lado do cliente:**
 - 2.6.2.3.1. Falsificação de conteúdo (spoofing);
 - 2.6.2.3.2. Cross-site Scripting:
 - 2.6.2.3.2.1. Cross-Site Scripting Refletido;
 - 2.6.2.3.2.2. Cross-Site Scripting Armazenado;
 - 2.6.2.3.2.3. Cross-Site Scripting DOM-based;
 - 2.6.2.3.3. Cross-Frame Scripting;
 - 2.6.2.3.4. HTML Injection;
 - 2.6.2.3.5. Falsificação de requisição Cross-Site;
 - 2.6.2.3.6. Ataques Relacionados a Flash:
 - 2.6.2.3.6.1. Cross-Site Flashing;
 - 2.6.2.3.6.2. Cross-Site Scripting através de Flash;
 - 2.6.2.3.6.3. Phishing/redirecionamento de URL através de Flash;
 - 2.6.2.3.6.4. Política cross-domain aberta.
 - 2.6.2.3.7. Ataques relacionados a aplicações padrão Web 2.0:
 - 2.6.2.3.7.1. Malicious AJAX Code Execution;
 - 2.6.2.3.7.2. XML Poisoning;
 - 2.6.2.3.7.3. RSS/Atom Injection;
 - 2.6.2.3.7.4. HTTP Request Splitting;
 - 2.6.2.3.7.5. WSDL Scanning e Enumeration;
- 2.6.2.4. Execução de Comando:**
 - 2.6.2.4.1. Ataque de Formato String;
 - 2.6.2.4.2. Injeção de LDAP;
 - 2.6.2.4.3. Injeção de comando de Sistema Operacional;
 - 2.6.2.4.4. SQL Injection;
 - 2.6.2.4.5. Blind SQL Injection;
 - 2.6.2.4.5. Injeção de SSI;
 - 2.6.2.4.6. Injeção de XPath ;
 - 2.6.2.4.7. Injeção de cabeçalho HTTP / Response Splitting;
 - 2.6.2.4.8. Inclusão de Arquivo remoto;
 - 2.6.2.4.9. Inclusão de Arquivo local;
 - 2.6.2.4.10. Uploads de arquivos potencialmente maliciosos;
- 2.6.2.5. Divulgação de Informações:**
 - 2.6.2.5.1. Estrutura de diretórios e arquivos;
 - 2.6.2.5.2. Vazamento de Informações:
 - 2.6.2.5.2.1. Informações sigilosas em comentários de código;
 - 2.6.2.5.2.2. Mensagens de erro de aplicação detalhadas;
 - 2.6.2.5.2.3. Arquivos de backup (default.old, index.bak, etc);
 - 2.6.2.5.2.4. Divulgação de arquivo de código fonte;

- 2.6.2.5.3. Path Traversal;
- 2.6.2.5.4. Localização de Recurso Previsível;
- 2.6.2.5.5. Métodos HTTP inseguros habilitados;
- 2.6.2.5.6. WebDAV habilitado;
- 2.6.2.5.7. Arquivos padrão de Servidor Web;
- 2.6.2.5.8. Páginas de Testes e Diagnósticos (test.asp, phpinfo.htm, etc.);
- 2.6.2.5.9. Extensões Front Page habilitadas;
- 2.6.2.5.10. Divulgação de endereço IP interno;

2.6.3. Customização de Teste

A solução de análise de segurança em aplicações Web deverá:

- 2.6.3.1. Permitir que o usuário modifique testes existentes;
- 2.6.3.2. Permitir ao usuário criar novos testes customizados;

2.6.4. Política de Teste

2.6.4.1. A solução de análise de segurança em aplicações Web deverá permitir ao usuário criar políticas de testes customizadas que especifiquem quais testes deverão compor uma análise;

2.6.5. Comprovação dos testes

2.6.5.1. A solução de análise de segurança em aplicações Web deverá facilitar a comprovação dos resultados apontados.

2.7. Gerenciamento da solução

2.7.1. Recursos de Controle de Varredura

2.7.1.1. A solução de análise de segurança em aplicações Web deverá possuir as seguintes capacidades de controle:

- 2.7.1.1.1. Agendar varreduras;
- 2.7.1.1.2. Pausar e continuar a análise;
- 2.7.1.1.3. Visualização em tempo real do status das varreduras em execução;
- 2.7.1.1.4. Definir modelos de configuração de varreduras reutilizáveis;
- 2.7.1.1.5. Executar varreduras simultaneamente;
- 2.7.1.1.6. Suportar múltiplos usuários;
- 2.7.1.1.7. Suportar varreduras remotas/distribuídas.

2.7.2. Interfaces de gerenciamento

2.7.2.1. A solução de análise de segurança em aplicações Web deverá fornecer as seguintes interfaces para administração e gerência da solução:

- 2.7.2.1.1. Aplicação Cliente com interface gráfica (GUI);
- 2.7.2.1.2. Interface de Linha de Comando (CLI).

2.7.3. Extensibilidade e interoperabilidade

2.7.3.1. A solução de análise de segurança em aplicações Web deverá possuir os seguintes recursos de extensibilidade e interoperabilidade:

- 2.7.3.1.1. API de varredura;
- 2.7.3.1.2. Capacidade de integração com sistemas de rastreamento de bugs comuns.

2.8. Relatórios

2.8.1. A solução deverá permitir a personalização do formato e das informações incluídas nos seus relatórios, fornecer todas as informações técnicas necessárias para que os usuários reproduzam os problemas identificados e habilidade de incluir:

- 2.8.1.1. Dados de requisição e respostas completos;
- 2.8.1.2. Lista de todos os Hosts e URLs incluídos na verificação.

2.9. Tipos de relatórios

A solução deverá fornecer os seguintes tipos de relatórios:

- 2.9.1.1. Resumo executivo;
- 2.9.1.2. Relatórios de detalhes técnicos.
- 2.9.1.3. Relatório histórico (diferencial entre duas análises de uma mesma aplicação);
- 2.9.1.4. Relatório de conformidade com as seguintes normas e padrões:

- 2.9.1.4.1. OWASP Top 10;
- 2.9.1.4.2. Classificação de ameaça WASC;
- 2.9.1.4.3. SANS Top 25;
- 2.9.1.4.4. Sarbanes-Oxley (SOX);
- 2.9.1.4.5. Payment Card Industry Data Security Standard (PCI DSS);
- 2.9.1.4.8. NIST 800-53.

2.10. Customização de Relatórios

A solução deverá fornecer a capacidade de customizar os seus relatórios, incluindo as seguintes:

- 2.10.1. Adicionar notas customizadas para as vulnerabilidades, que serão incluídas nos relatórios gerados;
- 2.10.2. Marcar as vulnerabilidades como falso-positivo e removê-las do relatório. De preferência, a solução deverá registrar quem marcou a vulnerabilidade como falso-positivo, quando, e as justificativas;
- 2.10.3. Ajustar o nível de risco de vulnerabilidades, incluindo:
 - 2.10.3.1. Nível de gravidade ou outros quantificadores de risco;
- 2.10.4. Identificar e reportar as vulnerabilidades de acordo com sua localização de conteúdo, que pode ser URLs, nome do Portlet, título da página, ou definido pelo usuário (por exemplo, um padrão de expressão regular na resposta);
- 2.10.5. Incluir customizações, como a adição de um logotipo da empresa ou modificação de rodapé do relatório e cabeçalho.

2.11. Formato de Relatórios

A solução deverá fornecer a capacidade de gerar relatórios, pelo menos, nos seguintes formatos:

- 2.11.1. PDF;
- 2.11.2. HTML;
- 2.11.3. XML.
- 2.11.4. Imagem (jpg, png);

2.12. Alertas para vulnerabilidade

2.12.1. A solução deverá ter capacidade para produzir alertas para cada tipo de vulnerabilidade específica que for identificada. Esses avisos deverão conter as seguintes informações:

- 2.12.1.1. Descrição da vulnerabilidade;
- 2.12.1.2. Nível de severidade;
- 2.12.1.3. Guia de remediação;
- 2.12.1.4. Exemplos de código de remediação.

2.13. Feedback ao fabricante

2.13.1. A solução deverá fornecer a capacidade de comunicar automaticamente falsos-positivos ou outros tipos de feedbacks para o fabricante do scanner para ajudar a melhorar a qualidade das versões futuras do produto. Esta informação deverá ser criptografada em trânsito e manipulada com segurança pelo fornecedor.

2.14. Da Quantidade

2.14.1. A solução de análise de segurança em aplicações web deverá ser fornecida em formato empresarial com licença para 10 usuários trabalharem simultaneamente, ou em formato individual, onde deverão ser entregues 10 licenças.

LOCALIDADE	QUANTIDADE
REGIONAL BRASÍLIA	06
REGIONAL RIO DE JANEIRO	01
REGIONAL SÃO PAULO	03

TOTAL	10
--------------	-----------

2.15. Da Operacionalização da Solução

2.15.1. Faculta-se o SERPRO e a Contratada, sempre quando necessário, agendar reuniões periódicas de caráter gerencial e/ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato e garantia.

2.15.2. O SERPRO se reserva no direito de remanejar a solução contratada entre suas Regionais e Escritórios, no Território Nacional.

2.16. Da Entrega e do Prazo de Entrega

2.16.1. Entende-se por cumprimento do prazo de entrega o recebimento dos componentes da solução, sua instalação e execução dos serviços no SERPRO, deixando-os operacionais para o aceite definitivo. O não cumprimento rigoroso do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada implicará em rescisão do contrato a ser firmado entre o SERPRO e a contratada.

2.16.2. A solução deverá ser entregue, instalada e configurada conforme solicitado no edital, de forma a estarem operacionais em até 30 (trinta) dias corridos a partir da assinatura do contrato.

2.17. Local de Instalação Inicial

2.17.1. A solução será operacionalizada na seguinte localidade:

REGIONAL BRASÍLIA/DF

ENDEREÇO: SGAN AV. L2 Norte, Quadra 601

Módulo "G"

CEP: 70836-900

TELEFONE: (61) 2021.9000

FAX: (61) 2021.9691

3.0 Níveis de Serviço

3.1. Suporte técnico à Solução ofertada

3.1.1. Possuir suporte técnico para a solução durante o período de vigência do contrato, assegurando prazos de atendimentos compatíveis com a instalação, no horário comercial (das 08h00min às 18h00min, de segunda-feira a sexta-feira, horário de Brasília), para um período de 48 (quarenta e oito) meses.

3.1.2. O atendimento aos chamados deverá obedecer a seguinte classificação quanto ao nível de severidade:

Severidade	Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução
1 – Média	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente.	Remoto, com exceção das situações em que seja necessária intervenção física.	No máximo 4 (quatro) horas após a abertura do chamado.	No máximo 10 (dez) horas após o início do atendimento do chamado.
2 – Baixa	Chamados com o objetivo de sanar dúvidas quanto ao uso ou à implementação	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.

	do produto.			
--	-------------	--	--	--

3.2. Chamados, Registros e Início de Prazos

3.2.1. Será aberto um chamado para cada problema reportado.

3.2.2. A abertura do chamado na CONTRATADA pelo SERPRO poderá ser realizado através de telefone e/ou WEB.

3.2.3. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado na CONTRATADA, recebendo dela uma identificação para acompanhamento, controle e histórico.

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

3.2.5. Tratamento dos chamados de Severidade 1

3.2.5.1. Os chamados de Severidade 1 serão atendidos em no máximo 4 (quatro) horas após a sua abertura e contarão com esforço concentrado da contratada com vistas a aplicar solução ou medida de contorno em até 10 (dez) horas após o início do atendimento do chamado.

3.2.5.2. Caso o problema não possa ser resolvido remotamente, a contratada deverá colocar à disposição do SERPRO, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema, sendo que o ônus financeiro de tal providência será da contratada.

3.2.5.3. O atendimento de Severidade 1 não poderá ser interrompido até o completo restabelecimento do produto envolvido, mesmo que se estenda por períodos noturnos e dias não úteis.

3.2.6. Tratamento dos chamados de Severidade 2

3.2.6.1. Os chamados de Severidade 2 serão atendidos em no máximo 24 (vinte e quatro) horas após a sua abertura e deverão ser concluídos em até 72 (setenta e duas) horas após a abertura do chamado.

3.2.6.2. Os chamados classificados com Severidade 2 serão atendidos em horário comercial, ou seja, das 08h00min às 18h00min, de segunda-feira a sexta-feira, horário de Brasília.

3.2.7. Manutenções

3.2.7.1. A CONTRATADA deverá prover, sempre que necessário, todas as correções e/ou atualizações dos softwares instalados que permitam melhorar suas funcionalidades, sem ônus adicional para o SERPRO.

3.2.7.2. Em qualquer hipótese a CONTRATADA deverá possuir acesso para suporte técnico de 2º nível, de forma a prestar os serviços de manutenção e assistência técnica, sem ônus adicional para o SERPRO. Para todos os efeitos da contratação em espécie, vigoram os seguintes conceitos:

3.2.7.3. Suporte Técnico Primeiro Nível: equipe treinada para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral.

3.2.7.4. Suporte Técnico Segundo Nível: escalonamento ao fabricante, devido à necessidade de retaguarda nas tecnologias suportadas.

3.2.8. Canais de atendimento

3.2.8.1. Atendimento através de canal telefônico gratuito 0800, em horário comercial.

3.2.8.2. Chamado técnico através de site na Internet, em horário comercial, e/ou canal telefônico gratuito 0800.

3.2.9. Escalação de Severidade

3.2.9.1 Por necessidade de serviço, o SERPRO poderá solicitar a escalação de chamado para níveis superiores de severidade. Os prazos dos chamados escalados passam a contar novamente do início.

3.2.10. Monitoramento do Atendimento dos Chamados

3.2.10.1. Todos os chamados serão controlados por sistema de informação da CONTRATADA.

3.2.10.2. Para efeito de acompanhamento das providências e do tempo decorrido desde a sua abertura, o SERPRO será informado sobre cada abertura e fechamento de chamado efetuado

por força da presente contratação.

3.2.10.3. O fechamento do chamado poderá se dar quer pela aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema.

3.2.10.4. A disponibilização de medida corretiva definitiva poderá, a critério da CONTRATADA, vir a ser incorporada em futuras versões do software.

3.2.10.5. Antes do fechamento de cada chamado a CONTRATADA consultará o SERPRO para validar o fechamento do chamado.

3.2.10.6. Um chamado fechado sem anuência do SERPRO ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

3.2.10.7. A CONTRATADA manterá cadastro das pessoas indicadas pelo SERPRO que poderão efetuar abertura e autorizar fechamento de chamados.

3.2.11. Relatórios sobre a Prestação dos Serviços

3.2.11.1. A CONTRATADA emitirá relatórios mensais referentes à prestação dos serviços, incluindo informações sintéticas dos chamados abertos e fechados, com ênfase para aqueles resolvidos no mês, informações sobre a disponibilização de novas versões e outras informações consideradas de relevância.

3.2.11.2. A CONTRATADA deve incluir nos relatórios no mínimo as informações do técnico do SERPRO responsável pela abertura do chamado, nível de severidade do chamado, a data e hora da abertura, data e hora do fechamento e solução aplicada.

3.2.12. Canais de atendimento

3.2.12.1. O atendimento será feito por meio do endereço web e/ou através de telefone gratuito 0800, a ser fornecido pela CONTRATADA quando da apresentação da proposta.

3.2.12.2. O atendimento deverá estar disponível em horário comercial.

3.3. Penalidades

3.3.1. A interrupção do atendimento de um chamado por parte da CONTRATADA, que não tenha sido previamente autorizada pelo SERPRO, ensejará aplicação de multa, conforme o nível de severidade do mesmo:

3.3.2. O não atendimento dentro do prazo estabelecido para o chamado ensejará aplicação de multa à contratada, conforme o nível de severidade do mesmo:

Severidade 1 – 0,10% (dez décimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

Severidade 2 – 0,05% (cinco centésimos por cento) do valor TOTAL da aquisição constante no contrato para o item (equipamento) correspondente, por hora ou fração de hora de atraso.

4.0 Especificação de Valores e Forma de Pagamento

4.1. O valor da aquisição está estimado em R\$.....

4.2. Local de Faturamento Inicial

4.2.1. A nota fiscal e/ou fatura deverão ser entregues em 2 (duas) vias, no Protocolo Geral do SERPRO, na localidade abaixo, onde será efetuado o pagamento, sendo:

4.2.1.1. Os itens descritos em 2.0 deverão ser entregues no seguinte endereço:

REGIONAL BRASÍLIA/DF

ENDEREÇO: SGAN AV. L2 Norte, Quadra 601

Módulo “G”

CEP: 70836-900

TELEFONE: (61) 2021.9000

FAX: (61) 2021.9691

INSCRIÇÃO ESTADUAL: 07334743/002-94

INSCRIÇÃO MUNICIPAL: 07334743/002-94

CNPJ: 33.683.111/0002-80

4.2.2. Constatando-se alguma incorreção na Nota Fiscal e/ou Fatura, o prazo para pagamento

será contado a partir da respectiva regularização. Carta de Correção só será admitida para regularizar os dados cadastrais do SERPRO. Deverá constar no corpo da nota fiscal e/ou fatura, o número do Contrato e do respectivo processo, além do banco, agência e número da conta onde deverá ser feito o pagamento;

4.2.3. A Razão Social do SERPRO na nota fiscal e/ou fatura deverá ser: SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO);

4.2.4. A Contratada deverá informar o CNPJ que será utilizado na emissão das notas fiscais e/ou faturas e e-mail;

4.2.5. Toda a solução deverá ser faturada com suas respectivas alíquotas de imposto;

4.2.6. Nos preços mencionados estão inclusas todas as despesas, tais como: taxas, impostos, frete, seguro, embalagens, manuais, despesas de transporte e garantia de funcionamento e atualização de versão dos programas, durante o período de 48 (quarenta e oito) meses;

4.2.7. Os pagamentos serão realizados nas regionais Brasília e Rio de Janeiro;

4.2.8. Todos os valores pertinentes aos serviços de instalação, configuração, níveis de serviço diferenciados por tratarem de obrigações da Contratada, deverão estar incorporados aos valores de cada item contratado.

5.0 Justificativa da Contratação

Não se aplica

6.0 Seleção do Contratado

O certame licitatório será através de Pregão Eletrônico, inicialmente pelo menor preço ofertado e a seleção da contratada dar-se-á nas seguintes condições:

6.1. Documentação e Homologação

6.1.1. A LICITANTE com a proposta de menor preço deverá apresentar em até 5 (cinco) dias úteis após solicitação do pregoeiro, documentação técnica do fabricante da solução comprovando o atendimento a todos os requisitos contidos na Especificação do objeto a ser contratado, bem como o atendimento das seguintes condições:

6.1.1.1. Documentação técnica do fabricante. Nessa documentação, a LICITANTE deve fornecer uma planilha ponto a ponto indicando documento e página onde consta o cumprimento de cada um dos requisitos das especificações técnicas;

6.1.1.2. Não serão aceitas referências a futuros releases ou versões de produtos para comprovar a existência ou aderência à qualquer quesito desta especificação;

6.1.1.3. Cada documento apresentado deve descrever claramente a referência ao modelo apresentado na proposta, não sendo válidas referências genéricas, e deverão seguir as formas de apresentação definidas na Especificação do Objeto;

6.1.1.4. Será aceita Carta do Fabricante, como comprovação de atendimento de requisitos técnicos e de compatibilidade especificados neste edital, apenas para os itens que não constarem na documentação da maioria dos fabricantes ou que não puderem ser mensurados;

6.1.1.5. Não será aceita Carta do Fornecedor, como comprovação de atendimento à requisitos técnicos e de compatibilidade especificados neste edital;

6.1.1.6. Relação de componentes, incluindo módulos, fontes e acessórios, de cada equipamento que compõe a solução, contendo o código do produto (fabricante) e as respectivas quantidades em cada item;

6.1.1.7. Caso, a documentação apresentada deixe de comprovar o atendimento de um único item da especificação técnica, a proposta será desclassificada, não passando para a etapa seguinte de testes das funcionalidades especificadas;

6.1.1.8. A proposta comercial a ser apresentada pela LICITANTE deverá discriminar os valores de todos os itens que compõem a solução ofertada, incluindo hardware, software e acessórios.

6.1.1.9. Avaliação prática, da EMPRESA LICITANTE CLASSIFICADA E APTA, em bancada de testes de características e funcionalidades exigidas nos itens da Especificação Técnica (2.0);

6.1.1.9.1. Esta etapa caberá à EMPRESA LICITANTE CLASSIFICADA E APTA, para todos os itens marcados como (AMOSTRA), comprovar na prática, através de testes de bancada, as características e funcionalidades exigidas, onde deverão ser utilizados equipamentos de homologação da EMPRESA LICITANTE CLASSIFICADA E APTA – não incorrendo em encargos

ao SERPRO;

6.1.1.9.2. Esta etapa será executada por prepostos do SERPRO em conjunto com os prepostos da EMPRESA LICITANTE CLASSIFICADA E APTA;

6.2. Toda homologação através de (AMOSTRA), deverá ser realizada nas dependências do SERPRO de Brasília;

6.3. Somente após a etapa de homologação será definida a EMPRESA LICITANTE VENCEDORA do processo licitatório.

6.3.1. Todos os testes e relacionamento dos técnicos da LICITANTE com o SERPRO deverão ser efetuados no idioma português;

6.3.2. Caso apenas um item referente às especificações seja considerado não atendido, a proposta será totalmente desclassificada;

6.3.3. A LICITANTE deverá indicar previamente os nomes de, no máximo, 6 (seis) técnicos para participação integral durante a realização dos testes de bancada e homologação. Esses técnicos deverão ser representantes legais da LICITANTE, comprovado através documentação de vínculo contratual ou procuração;

6.3.4. A LICITANTE deverá indicar previamente os nomes dos seus técnicos responsáveis pela instalação dos equipamentos nas dependências do SERPRO em número a ser definido pela proponente.

6.3.5. A critério da LICITANTE, as etapas do aceite poderão ser acompanhados por técnico do fabricante;

6.3.6. Dos técnicos indicados pela LICITANTE, apenas um poderá ser substituído após o início dos testes de bancada, desde que seja comunicado formalmente ao SERPRO;

6.3.7. As empresas concorrentes do pregão poderão indicar técnicos (apenas um para cada empresa) para acompanhar os testes de bancada. As indicações deverão ser realizadas com, no mínimo, 2 dias de antecedência e apenas serão permitidos questionamentos diretos aos técnicos do SERPRO;

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

6.3.9. Durante a realização dos testes de bancada serão permitidas atualizações de software sob avaliação, visando a correção ou adaptação para atendimento aos requisitos do edital. Essas atualizações poderão corrigir mais de um item simultaneamente;

6.3.9.1 A critério do Serpro os testes de bancada poderão ser reiniciados após atualização de versão;

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

6.3.11. A modalidade para realização da aquisição será pregão eletrônico e a adjudicação será pelo menor valor global.

6.4. Homologação da Solução

6.4.1. Após aceite da documentação comprobatória, a LICITANTE deverá disponibilizar para a realização das etapas de homologação, no prazo de até 30 (trinta) dias corridos contados à partir da solicitação do pregoeiro, amostra da mesma marca e modelo ofertado na proposta, conforme especificação do objeto;

6.4.2. A LICITANTE deverá disponibilizar adicionalmente todos os demais equipamentos necessários para a realização dos testes de bancada;

6.4.3. O SERPRO fornecerá um prazo de 10 (dez) dias úteis para a realização da fase de homologação;

6.4.4. O prazo de homologação poderá ser prorrogado por igual período a critério do SERPRO.

7.0 Justificativa para Aceitação de Preços

Não se aplica

8.0 Gerenciamento do Contrato

8.2. Da Operacionalização da Solução

8.2.1. Faculta-se o SERPRO e a Licitante, sempre quando necessário, agendar reuniões periódicas de caráter gerencial e/ou técnico para avaliar os trabalhos, adotar resoluções e obter esclarecimento de pendências durante toda a vigência do contrato e garantia;

8.3. O SERPRO se reserva no direito de remanejar a solução contratada entre suas Regionais e Escritórios, no Território Nacional;

8.4. Entende-se por cumprimento do prazo de entrega o recebimento dos componentes da solução, sua instalação e execução dos serviços no SERPRO, deixando-os operacionais para o aceite definitivo. O não cumprimento rigoroso do prazo de entrega, ou entrega parcial, ou entrega de configuração inferior a solicitada implicará em rescisão do contrato a ser firmado entre o SERPRO e a contratada;

8.5. O SERPRO se reserva no direito de utilizar a solução contratada para utilização interna e para atender possíveis demandas dos clientes, respeitando a forma de uso e quantitativo das licenças adquiridas para esta finalidade;

8.6. Repasse de Conhecimento

8.6.1 Como parte integrante do processo de instalação, configuração, implantação, implementação e produção, a empresa vencedora deverá realizar o repasse de conhecimento para o SERPRO, dos conhecimentos necessários para instalar, administrar, configurar, operar, desenvolver e gerenciar os produtos fornecidos.

8.6.2. O repasse de conhecimento para o SERPRO deverá ser iniciado em até 30 (trinta) dias após o aceite da solução, podendo ser adiada por conveniência do SERPRO, quando então, em comum acordo com a CONTRATADA, será marcada a data definitiva.

9.0 Considerações Gerais

9.1. O prazo de vigência do contrato será de 12 (doze) meses, contado a partir da data de assinatura;

9.2. O prazo de garantia dos produtos ofertados para cada item da especificação técnica será de 48 (quarenta e oito) meses;

9.3. A empresa Licitante deverá apresentar documento(s) que comprove(m) a aptidão técnica necessária para executar o objeto, tais como contrato, termo, certificado, declaração, endereço eletrônico de sítios oficiais do fabricante na internet, entre outros documentos pertinentes que demonstrem de forma inequívoca, a habilidade técnica para prestar o serviço de suporte técnico e vínculo vigente com o fabricante do hardware e do software;

9.4. Não haverá necessidade de apresentação da declaração prevista no item 9.3, quando a licitante for a própria fabricante do hardware e software;

9.5. O objeto da presente contratação está caracterizado como bens ou serviços de informática ou automação, conforme definição constante no Art. 16-A da Lei nº 8.248, de 23 de outubro de 1991;

9.6. Os serviços especificados possuem características de serviços contínuos, sem dedicação exclusiva de mão de obra;

9.7. A Ata de Registros de Preços a ser criada será de uso exclusivo do Serpro em toda sua capilaridade geográfica.

Elaboração

Data:

EDUARDO LIMA - 12005240

COGTI/CIPOA