



**SERVIÇO PÚBLICO FEDERAL  
MJ – DEPARTAMENTO DE POLÍCIA FEDERAL  
COORDENAÇÃO-GERAL DE TECNOLOGIA DA INFORMAÇÃO**

**ANEXO I**

**1. QUANTITATIVOS**

1.1 Os seguintes serviços compõem a solução em licitação por LOTE ÚNICO:

Item	Descrição	Quantidade	Prazo
1	Renovação de licença de gateway de segurança WEBSense "Web Filter & Security" para 15.000 usuários.	01 licença	12 meses
2	Serviço de suporte técnico, atualização de versão, correção de bugs (segunda a sexta).	01 serviço	12 meses
3	Banco de 200 (duzentas) horas para implementação de melhorias na solução de segurança.	200 horas	12 meses

1.2 A justificativa da relação entre a demanda e a quantidade de serviço a ser contratada, nos termos do art. 15, §7º, inc. II, da IN nº 02/08 SLTI – MPOG, consta da Informação nº 1400311/2017-SST/DINF/CGTI/DLOG/PF, parte integrante dos autos.

**2. REQUISITOS – ESPECIFICAÇÃO TÉCNICA**

**ITEM 1 - Serviço de gateway de segurança para 15.000 (quinze mil) usuários. Requisitos obrigatórios da ferramenta que devem ser mantidos durante a vigência contratual:**

2.1 A PROPONENTE Deve fornecer uma proposta para licenciamento de uso do software WEBSense durante 12 meses na modalidade "Web Filter & Security" para 15.000 (quinze mil) usuários.

2.2 Aplicar políticas de filtro de conteúdo Web combinando categorias de sites, categorias de protocolos, clientes e horário de acesso.

2.3 Possuir, no mínimo, as seguintes categorias de URL's:

- 2.3.1 Ameaças de segurança (bot-networks, vírus, phishing, spyware, embedded-links, embedded-iframe, hackers, keyloggers, malwares, proxies públicos, sites comprometidos)
- 2.3.2 Armas
- 2.3.3 Banners e publicidade
- 2.3.4 Compras
- 2.3.5 Controle de banda (vídeo, áudio, compartilhamento de arquivos, online streaming)
- 2.3.6 Downloads de softwares
- 2.3.7 Drogas ou Narcóticos
- 2.3.8 Educação
- 2.3.9 Esportes
- 2.3.10 Ferramentas de colaboração
- 2.3.11 Notícias
- 2.3.12 Redes sociais
- 2.3.13 Veículos
- 2.3.14 Viagens

2.4 Possuir mais de 60 milhões de URL's em sua base de dados de classificação.

**2.5** Permitir nova categorização de sites por URL's específicas ou por expressões regulares, segundo as necessidade da PF, independente da definição do fabricante.

**2.6** Possuir a capacidade de detectar tráfego de rede não-HTTP e bloquear tais protocolos através das políticas definidas.

**2.7** Possuir mais de 100 tipos de protocolos não-HTTP em sua base de dados de classificação.

**2.8** Possuir, no mínimo, as seguintes categorias de protocolos:

- 2.8.1** Correio eletrônico (POP3, SMTP, IMAP)
- 2.8.2** Tráfego P2P (Kazaa, Morpheus, BitTorrent, eDonkey, Gnutella, Qnext, WinMX, DirectConnect)
- 2.8.3** Telefonia IP (Skype)
- 2.8.4** Evitação de Proxy (Hopster, GhostSurf, Google Web Accelerator, JAP, RealTunnel, Tor, Your Freedom)
- 2.8.5** Ferramentas controle remoto (Citrix, GoToMyPC, LogMeIn, pcANYWHERE, Windows Terminal Services, VNC, WebEx)
- 2.8.6** Protocolos de streaming de mídia (AOL Radio, Google Video, iTunes, JetCast, Liquid Audio, PeerCast, QuickTime, SHOUTcast, Windows Media)

**2.9** Fornecer integração com um ou mais serviços de diretórios de usuários (Microsoft Active Directory) a fim de identificar de modo transparente os clientes (usuários) e aplicar a política definida individualmente ou por grupo.

**2.10** Fornecer compatibilidade com autenticação LDAP, Radius e NTLM.

**2.11** Não deve haver limitação na aplicação de políticas entre diferentes usuários, caso seja necessário bloquear um acesso e liberar outro.

**2.12** Os acessos bloqueados pela ferramenta devem ser informados ao cliente através de uma página específica, customizável.

**2.13** No caso dos acessos com período definido (cota de tempo), deve exibir mensagem de confirmação para a contagem do tempo de acesso do usuário.

**2.14** Deve ser capaz de realizar integração nativa com ativos de rede, sendo no mínimo os seguintes:

- 2.14.1** Firewalls (Cisco FWSM Firewall, Cisco ASA, Check Point Firewall-1 NG, CyberGuard, NetScreen/Juniper, SonicWall, ServGate, 3Com SuperStack Firewall)
- 2.14.2** Proxies (SunONE Web Proxy Server, Squid Stable 2.5, Websense Content Gateway)
- 2.14.3** Sistemas de Cache (Blue Coat ProxySG, Network Appliance NetCache, 3Com Webcache, Cisco Content Engine, Cisco Network Module, iMimic DataReactor, Inktomi Traffic Server, Stratacache Flyer)
- 2.14.4** Roteadores e switches (Cisco Routers, Cisco Catalyst Swiches)
- 2.14.5** Possuir console de administração única para prover gerenciamento das políticas, clientes e emissão de relatórios.

**2.15** Manter registro para fins de auditoria de cada modificação feita por cada Administrador nas políticas e configurações da solução.

**2.16** Registrar os acessos em banco de dados relacional centralizado, com mecanismos de manutenção e de armazenamento off-line dos períodos antigos.

**2.17** Registrar em cada acesso: identificação do cliente, data e hora do acesso, url acessada, método HTTP, tamanho da requisição.

**2.18** Prover funcionalidade de programação periódica de emissão de relatórios pré-definidos por email ou pasta de rede.

**2.19** Permitir emissão de relatórios por categorias acessadas, por usuário, por riscos de segurança, por faixas de endereço IP.

- 2.20** Permitir exportar os relatórios em diferentes formatos (PDF, XLS, HTML).
- 2.21** Deve suportar clustering e permitir a criação de um endereço IP virtual para garantir alta disponibilidade da solução.
- 2.22** Possuir a funcionalidade de Proxy Web, suportando os protocolos HTTP, HTTPS e FTP.
- 2.23** Permitir a configuração de portas diferentes das padrões para cada um dos protocolos suportados.
- 2.24** Deve ser capaz de atuar como um proxy explícito e transparente através do protocolo WCCP.
- 2.25** Deve criar e hospedar arquivos PAC (Proxy Auto Configuration) e WPAD (Web Proxy Auto Discovery).
- 2.26** Deve permitir ser um membro de uma hierarquia de cache HTTP e ICP (Internet Cache Protocol).
- 2.27** Deve suportar o armazenamento de conteúdo HTTP e FTP em cache.
- 2.28** Deve possuir mecanismo para descriptação do tráfego SSL para fins de inspeção do conteúdo acessado.
- 2.29** Permitir a configuração de categorias ou sites isolados para que o tráfego SSL não seja descriptografado.
- 2.30** Permitir a configuração de endereços IP de origem ou range IP de origem não tenham seu tráfego SSL inspecionado.
- 2.31** Permitir o uso da console de gerenciamento por usuários com perfil limitado, sem administração e somente emissão de relatórios.
- 2.32** Suportar o uso de Appliance Websense V. 10.000, servidores virtualizados e servidores dedicados.
- 2.33** Deve permitir que os serviços sejam instalados em diferentes equipamentos para fins de performance e escalabilidade, inclusive Deve permitir que certos serviços sejam instalados sobre sistemas operacionais diferentes.
- 2.34** O uso de servidores distribuídos não deve gerar custos adicionais de licenciamento. Estando este, vinculado apenas à quantidade de usuários suportados.
- 2.35** Deve suportar conexões de protocolo SOCKS, permitindo o tunelamento de aplicativos que não sejam compatíveis com Proxy.
- 2.36** Deve suportar o protocolo de comunicação IPV6.

## **ITEM 2 – Suporte técnico 8x5x48**

- 2.37** A PROPONENTE deve fornecer uma proposta para contratação de suporte técnico especializado oferecido por telefone, correio eletrônico e acesso remoto via Internet para todos os componentes da solução de gateway de segurança WEBSense.
- 2.38** O serviço de suporte técnico especializado deve estar disponível de segunda à sexta-feira, das 08:00 horas às 18:00 horas, através de uma Central de Atendimento, que disponibilize pelo menos um endereço de correio eletrônico (e-mail) e um número de telefone 0800 (ligação gratuita) como canal de acionamento para suporte técnico remoto durante toda a vigência do contrato.
- 2.39** A solução de acesso remoto deve ser custeada pela CONTRATADA e prever o acesso compartilhado entre o seu corpo técnico e um representante da PF aos equipamentos da solução WEBSense.
- 2.40** Cada ocorrência aberta na Central de Atendimento da CONTRATADA, deve gerar um número de registro e um e-mail para um endereço interno da CONTRATANTE, contendo informações sobre o ticket para o acompanhamento do chamado.
- 2.41** O prazo para início de atendimento remoto é de 5 (cinco) minutos na fila de espera do atendimento telefônico ou 1 (uma) hora para resposta via e-mail.

**2.42** A CONTRATADA deve fornecer uma página WEB que permita à CONTRATANTE acompanhar o status dos chamados abertos e emitir relatório de chamados por data de abertura, contendo ao menos as informações de data de fechamento, assunto e status para cada registro.

**2.43** As atividades envolvidas nos acionamentos de suporte técnico devem compreender:

- 2.43.1** Suporte corretivo – correção de bugs e/ou falhas e quaisquer atividades que tenham por finalidade restabelecer o normal funcionamento da solução.
- 2.43.2** Suporte preventivo – atualização dos softwares, por meio de patches; alerta e correção de possíveis incompatibilidades detectadas; recomendação de configurações consoante às melhores práticas do produto.
- 2.43.3** Esclarecimento de dúvidas – questionamentos de natureza técnica relativos à solução e ao seu ambiente de operação, bem como sobre a instalação, configuração, manutenção e operacionalização da solução, e a instalação, desinstalação e atualização de software.
- 2.43.4** Avaliação de desempenho – análise de situações em que o serviço esteja disponível, mas a experiência do usuário não seja satisfatória. Auxílio na identificação de pontos de limite do desempenho da ferramenta perante todos ou parte dos clientes, proposição de ajustes, bem como emissão de parecer técnico.

**2.44** Durante a vigência do contrato, as novas versões e os “releases” dos softwares deverão ser disponibilizados pela CONTRATADA e instalados sem quaisquer ônus para a PF.

**2.45** Mensalmente, deverá ser realizada ao menos uma sessão remota com objetivo de realizar verificação em todos os componentes da solução de segurança WEBSense, sob o aspecto de identificação de eventuais alertas, aplicação de pequenas correções e avaliação de conformidade com a política de segurança.

### **ITEM 3 – Banco de horas para implementação de melhorias**

**2.46** A proponente deve fornecer uma proposta para contratação de um banco de até 200 horas para utilização sob demanda, com o valor medido por hora, durante a vigência do contrato.

**2.47** O quantitativo de horas acima especificado é estimativo e não implica obrigação de utilização. O pagamento somente será realizado contra as horas efetivamente utilizadas.

**2.48** Apenas o período em que o técnico estiver presente no local solicitado pela Polícia Federal poderá ser contabilizado do banco de horas.

**2.49** As seguintes atividades podem ser solicitadas para a CONTRATADA:

- 2.49.1** Manutenção evolutiva para integração de soluções.
- 2.49.2** Apoio nas definições do produto para composição de soluções.
- 2.49.3** Suporte no desenvolvimento de soluções que utilizem o produto.
- 2.49.4** Avaliações, diagnósticos e proposições de soluções de melhoria.
- 2.49.5** Geração de relatórios de vistoria e análise.
- 2.49.6** Implementações adicionais.
- 2.49.7** Alteração da configuração nos equipamentos.
- 2.49.8** Workshops de conscientização de usuários e administradores da ferramenta.
- 2.49.9** Outras atividades relacionadas com a solução entregue.

**2.50** O pagamento das horas utilizadas será realizado mensalmente, mediante discriminação no documento de cobrança do total das horas efetivamente utilizadas no mês de referência.

**2.51** O pagamento das horas utilizadas será realizado mensalmente, mediante discriminação no documento de cobrança do total das horas efetivamente utilizadas no mês de referência.

**2.52** A utilização das horas deve ser formalizada pela CONTRATANTE através de e-mail ou em formato a ser acordado.

**2.53** Ao final de cada atendimento do banco de horas, deverá ser preenchido pela CONTRATADA um relatório técnico descrevendo as atividades realizadas, data e hora do início e término do atendimento, assinatura do representante da CONTRATANTE e pelo representante da CONTRATADA durante o atendimento.

**2.54** O local da prestação do banco de horas poderá ser qualquer uma das unidades na Polícia Federal no território nacional, conforme indicação da CONTRATANTE.

### 3. TRANSFERÊNCIA DE TECNOLOGIA

**3.1** A presente contratação visa manter a continuidade de serviços atualmente prestados, portanto, não há necessidade de transferência de tecnologia.

### 4. NÍVEIS DE SERVIÇO E PENALIZAÇÕES

**4.1** A CONTRATADA deverá atender aos Níveis de Serviços apresentados na tabela a seguir, com prazos definidos segundo a severidade do chamado/solicitação:

Severidade	Descrição	Prazo máximo para resposta inicial	Prazo máximo para restauração do serviço	Prazo máximo para solução definitiva
1 - Alta	<p>Indisponibilidade do produto ou componente essencial para o funcionamento da solução de segurança.</p> <p>O item afetado impacta na aplicação das políticas ou na disponibilidade do acesso à Internet.</p> <p><u>Exemplos:</u></p> <ul style="list-style-type: none"> <li>- Servidor está ativo, mas componente de filtragem não está funcionando.</li> <li>- Servidor está ativo, mas componente de identificação dos usuários está inativo.</li> <li>- A solução afeta operações relacionadas ao negócio da Polícia Federal.</li> </ul>	Em até 15 minutos deve ser realizada sessão remota para solucionar o problema.	Até 8 (oito) horas.	Até 6 (seis) dias.
2 - Média/Alta	<p>Grande restrição de funcionalidade da solução de segurança.</p> <p><u>Exemplos:</u></p> <ul style="list-style-type: none"> <li>- Servidor ou componente está indisponível, mas existe redundância atendendo o serviço.</li> <li>- Servidor está ativo, mas componente de registro dos acessos não está funcionando.</li> <li>- Servidor está ativo, mas a console de administração não está funcionando.</li> </ul>	Em até 02 horas deve ser realizada sessão remota para solucionar o problema.	Até 24 (vinte e quatro) horas.	Até 10 (dez) dias.
3 - Média/Baixa	<p>Incompatibilidade de uma nova aplicação com a solução de segurança. Demandas de suporte preventivo.</p> <p><u>Exemplo:</u></p> <ul style="list-style-type: none"> <li>- A conexão com a Internet de uma aplicação específica não está funcionando adequadamente.</li> </ul>	Em até 06 horas deve ser realizada sessão remota para solucionar o problema.	----	Até 15 (quinze) dias e/ou na próxima atualização de software.

4 - Baixa	<p>Esclarecimentos de dúvidas, parecer técnico, documentação.</p> <p><u>Exemplo:</u></p> <ul style="list-style-type: none"> <li>- Elaboração de documentação sobre a infraestrutura.</li> <li>- Encaminhamento de sugestões ou pedidos de novos recursos</li> </ul>	No próximo dia útil	----	Até 20 (vinte) dias ou considerado para as próximas atualizações de software.
-----------	---	---------------------	------	---

**4.2** Em caso de não atendimento por parte da CONTRATADA de prazos definidos na tabela de Nível de Serviços (item anterior), devem ser aplicadas as penalizações à CONTRATADA definidas na tabela a seguir, até o limite mensal de 30% do valor mensal do Contrato, sem prejuízo das demais sanções contratuais:

Criticidade	Descrição
1 – Alta	1,00 % do valor mensal do contrato por cada hora que exceder o prazo de 8 (oito) horas para a restauração do serviço.
	0,50 % do valor mensal do contrato por cada dia que exceder o prazo de 6 (seis) dias para o fornecimento de solução mais completa e/ou permanente para o problema.
2 – Média/Alta	0,60 % do valor mensal do contrato por cada hora que exceder o prazo de 24 (vinte e quatro) horas para a restauração do serviço.
	0,30 % do valor mensal do contrato por cada dia que exceder o prazo de 10 (dez) dias para o fornecimento de solução mais completa e/ou permanente para o problema.
3 – Média/Baixa	----
4 – Baixa	----

**4.3** Não serão computados nos prazos para a resposta a incidentes nas soluções contratadas previstos na tabela do item 4.1 o tempo dispendido em ações necessárias para viabilizar o atendimento que sejam de responsabilidade exclusiva do CONTRATANTE.