CONSULTA PÚBLICA Nº 002/2015

A Secretaria de Estado da Fazenda - SEFAZ realizará oportunamente processo de licitação visando à aquisição de solução de TI – Secure Web Gateway, serviço de instalação e treinamento, no âmbito do Plano de Desenvolvimento da Administração Fazendária – PROFAZ ES, financiado com recursos do Banco Interamericano de Desenvolvimento - BID.

Tendo em vista a necessidade de verificar a compatibilidade das especificações com o que é usualmente contratado no mercado, além de estabelecer critérios de paridade de preços, segundo o art. 3º da Lei nº 8.666/93, e de isonomia entre os fornecedores, bem como de esclarecer eventuais dúvidas, a Secretaria de Estado da Fazenda - SEFAZ submete à Consulta Pública, **no período de 27/07/2015 a 12/08/2015**, as Especificações Técnicas elaboradas pela área de Tecnologia da Informação, permitindo aos interessados a apresentação de seus questionamentos, sugestões e orçamentos estimativos.

Os questionamentos, sugestões e orçamentos estimativos, deverão ser encaminhados por escrito até a data final da consulta, exclusivamente, para o endereço de correio eletrônico cplprofaz@sefaz.es.gov.br. As respostas aos questionamentos serão publicadas na página correspondente a esta Consulta Pública, no seguinte sítio da Internet: www.sefaz.es.gov.br/profaz (opção Licitações / Aquisições).

Ressaltamos que os valores de orçamentos estimativos eventualmente apresentados pelos interessados, que deverão seguir o formato previsto no Anexo I a seguir, terão a única finalidade de servir de parâmetro para a estimativa de preço para a licitação a ser realizada.

RICARDO ISHIMURA
Pregoeiro Oficial
CPL/PROFAZ

PARTE 1 – IDENTIFICAÇÃO DO PROJETO

1.1 TÍTULO DO PROJETO

Aquisição de solução de TI – Secure Web Gateway.

1.2 OBJETIVO

Aquisição de solução de TI – Secure Web Gateway, serviço de instalação e treinamento.

1.3 MODALIDADE DE CONTRATAÇÃO SUGERIDA

De acordo com a legislação vigente.

1.4 ESTIMATIVA DE CUSTO GLOBAL

- De acordo com a legislação vigente.

1.5 PRAZO ESTIPULADO PARA O CONTRATO

O contrato de manutenção, suporte e garantia dos equipamentos deve ser de 12(doze) meses, contados após a conclusão das etapas de homologação e entrega final.

1.6 UNIDADE ADMINISTRATIVA RESPONSÁVEL PELA COORDENAÇÃO DO PROJETO

O projeto tem como unidade administrativa responsável a Secretaria da Fazenda do Estado do Espírito Santo sendo gerido, pela Gerência de Tecnologia da Informação – GETEC.

PARTE 2 – CONTEXTUALIZAÇÃO

2.1 BENEFÍCIOS DOS PRODUTOS

O Produto Secure Web Gateway trará uma serie de benefícios para os usuários nos quais destacamos a seguir:

- Filtro de Conteúdo - Os usuários poderão navegar com segurança nos sites que terão sua categorização em tempo real evitando assim acesso a sites indesejados.

- Antivírus - Todos os sites e arquivos serão filtrados pelo antivírus do Secure Web Gateway antes de serem carregados nos computadores dos usuários.

- Priorização de Aplicações - As aplicações e serviços prioritários que utilizam a internet poderão ter uma prioridade maior que os outros serviços, tendo assim uma velocidade de internet maior que os serviços comuns.

- Balanceamento - Todo acesso a internet será de modo redundante e balanceado aumentando assim a disponibilidade do serviço de internet.

- Aplicações web 2.0 - Será possível habilitar/filtrar as aplicações web 2.0 tais como: facebook, youtube, entre outras onde será possível liberar o acesso às funções especificas de cada site.

- Cache - Aumenta o tempo de resposta e desempenho no acesso à internet e também economia de banda de internet já que o conteúdo dos sites será armazenado localmente.

- Relatórios/Logs - Será possível gerar diversos tipos de relatórios no qual destacamos: Relatórios por usuário, por sites, por banda consumida e também acesso aos logs de conexão que serão de suma importância de resolução de problemas de acesso.

- Suporte 24x7 - Agilidade na resolução de problemas de acesso à internet.

PARTE 3 – OBJETIVO GERAL DO PROJETO

3.1 JUSTIFICATIVA

A solução de proxy (acesso a internet) atualmente em utilização pela SEFAZ “Fortigate” do fabricante Fortinet, já não consegue atender a demanda de acesso a internet requisitada pelos usuários desta Secretaria.

Dentro deste contexto, a SEFAZ necessita modernizar sua estrutura de acesso à internet, adquirindo uma solução de Secure Web Gateway.

3.2 EVIDENCIAR CLARAMENTE O INTERESSE PÚBLICO DA CONTRATAÇÃO DOS BENS E SERVIÇOS PREVISTOS NO PROJETO BÁSICO

O projeto em questão, pretende dar maior segurança, disponibilidade, priorização de aplicações e isso trará uma série de benefícios no atendimento aos contribuintes.

As primícias do referido processo é fornecer ao cidadão público um serviço eficiente e eficaz, visando uma máquina estatal mais eficiente. A execução nas repartições públicas, de forma geral, reclama por melhorias nas instalações físicas, mais tecnologia, capacitação e valorização da atividade. A imagem organizacional precisa ser fortalecida através da prestação de um atendimento moderno, rápido e confiável. Para tanto, faz-se necessária melhorias estruturais, tecnológicas e de gestão ao processo de atendimento da SEFAZ.

3.3 PRAZO ESTIMADO PARA ALCANÇAR O RESULTADO ESPERADO

Após a instalação e configuração do equipamento no ambiente da SEFAZ o resultado esperado será imediato.

PARTE 4 – PRODUTOS E SERVIÇOS A SEREM CONTRATADOS

Esta especificação estabelece as características técnicas mínimas para fornecimento dos produtos descritos neste projeto, incluindo serviços de manutenção e garantia “on-site” pelo período de 36 (trinta e seis) meses.
Aquisição de solução de TI para as unidades da SEFAZ, solução de SWG – Secure Web Gateway, conforme a seguir.

LOTE 1 – ITEM 1 – AQUISIÇÃO DE SOLUÇÃO DE SWG – SECURE WEB GATEWAY

4.1.1. Aquisição de solução SWG – Secure Web Gateway, conforme especificações técnicas abaixo:

- **a. QUANTIDADE: 2(dois).**
- **b. PRAZO DE ENTREGA: EM ATÉ 30 DIAS APÓS A ASSINATURA DO CONTRATO.**
- **c. SOLUÇÃO SWG, CONFORME ESPECIFICAÇÕES:**
  - **1. DESEMPENHO, CAPACIDADE E ALTA DISPONIBILIDADE:**
    a. A solução deverá prover as funcionalidades de Proxy HTTP/HTTPS, Filtro de Conteúdo, Caching e AntiMalware, incluindo e inspeção de tráfego SSL e Monitoramento de camada quatro do modelo OSI;

    b. Todas as funcionalidades especificadas dos equipamentos devem estar aptas e licenciadas no ato de sua aquisição, sem custos adicionais para sua plena utilização. Caso ocorra a necessidade de instalação de Patch’s e atualização de Firmware os mesmos não poderão afetar as funcionalidade exigidas neste edital.

    c. Deve prover o serviço para no mínimo 700 usuários simultâneos.

d. Deve prover armazenamento temporário de objetos (cache) e ainda permitir que seja definido o tamanho máximo de objetos.

e. Deve ser fornecido em formato appliance, portanto com hardware dedicado ao seu funcionamento. O appliance deve ser fornecido com no mínimo 03 (três) interfaces 10/100/1000BaseT sendo uma destas dedicada ao gerenciamento da solução.

f. O equipamento oferecido deve permitir o adicionamento de licenças para até 3500 usuários sem a necessidade de upgrades físicos.

g. Deve suportar a montagem em Rack de 19".

h. Deve ser composta por dois equipamentos em cluster Ativo-Ativo e Ativo-Passivo com processamento e alimentação individual, de maneira que caso ocorrendo uma parada ou defeito parcial de um dos equipamentos não interfira de modo algum no funcionamento da solução, sendo um dos nós capaz de suportar a capacidade total exigida para a solução, bem como licenciamento.

i. Caso a os equipamentos não executem a função de gerenciamento unificado e emissão de relatórios, serão admitidas máquinas virtuais compatíveis com o ambiente virtualizado de nossa secretaria, a saber: VSphere 5.5 ou superior.

j. A solução deve permitir a configuração manual e automática de horário através de uso NTP ou SNTP.

k. Possuir latência de no máximo 15 milissegundos.

l. Possuir suporte a implementação e compatibilidade a IPv6, bem como a ICMPv6(RFC 4890) de forma a permitir a criação de políticas baseadas no ICMP Type.

m. Possuir quantidade de memória e capacidade de processamento necessários ao seu funcionamento pleno com todas as funcionalidades descritas nesta especificação e com desempenho adequado.

2. GERENCIAMENTO:

a. Deve possuir capacidade de integração com Serviço de Diretório Windows, possibilitando o gerenciamento e administração da ferramenta com base nas informações deste serviço.

b. A autenticação deve ser baseada em ao menos dois dos quatro seguintes protocolos: NTLM, kerberos, ldap, radius. A autenticação via NTLM deve ocorrer de modo transparente, ou seja, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha de acesso (Single Sign-On).

c. A autenticação de usuários e estações de trabalho deve ocorrer sem a necessidade de instalação ou execução de clientes ou quaisquer módulos em nenhuma estação de trabalho ou servidor.

d. A capacidade para gerência e administração da ferramenta deve possibilitar a concessão de direitos a usuários e grupos com no mínimo três níveis de privilégios, como por exemplo: Administrador, operação e emissor de relatórios.

e. Todas as operações da solução deverão ser executadas em console único, e somente será admitida a necessidade de acesso a outros consoles, para tarefas de manutenção da ferramenta.

f. Deve possuir gerenciamento gráfico (web) do equipamento via protocolo HTTP ou HTTPS de forma intuitiva e amigável (point-and-click), possibilitando todo gerenciamento tal como: Criação de políticas, resolução de problema e acesso a relatórios sem a necessidade da CLI (Command Line Interface) ou semelhante, como, por exemplo, CLI HTTP;

g. Deve possuir auditoria de configuração, gravando e disponibilizando todas as alterações que identifique no mínimo: Quem, Quando e o que foi alterado.

h. Deve permitir a execução cópias de segurança (backup) de forma manual e automática, e permitir também a restauração destas cópias.

i. Deve implementar os padrões abertos de gerência de rede SNMPv1, SNMPv2c e SNMPv3, incluindo a geração de traps;

3. CONTROLE DE APLICAÇÕES:

a. Deve permitir a criação de regras que possibilite a permissão ou bloqueio de aplicações diversas tais como:

- Entretenimento: IM, proxy anônimo e similares.
- Acesso remoto: Logme-in, Team Viewer, VNC e similares.
- Potenciais consumidores de banda: P2P, Média Players e similares.

b. Suportar os protocolos HTTP, HTTPS e FTP, em seus modos ativo e passivo;

4. FILTRO DE ACESSO:

a. Deve permitir a criação de regras que possibilite a permissão ou bloqueio de acesso baseado nos seguintes critérios:

- Origem (Grupos do domínio ou serviço de diretórios LDAP e AD ao qual o usuário pertence; Aplicação);
- Destino (Categoria, domínio, url/lista);
- Tipo de arquivo;

- Protocolos (HTTPS, FTP e outros);
- Horário (definir períodos de funcionamento por regra);

b. Deve permitir definição de largura ou porcentagem de banda máxima para o acesso de acordo com o estabelecido em regra, baseando-se em categoria do destino ou protocolo.

c. A solução deve atuar como *"man in the middle"*, intermediando e repassando todas as requisições. Deve suportar certificados on-box, importando certificados validos ou gerando auto-assinados. Deve permitir a emissão de páginas amigáveis e customizáveis de erro também aos sites criptografados.

d. Deve Permitir o controle de acesso através do percentual de largura de banda disponível para determinadas Categorias e os limites de banda devem ser definidos por:

   - Limite geral ou percentual de Banda - Definindo um limite global para todos os usuários da rede para os tipos de aplicativos para definir um limite global de largura de banda para restringir a quantidade de tráfego de rede.
   - Limite de Banda por Usuário. Definindo um limite para determinados usuários na rede por categoria, definindo os limites de largura de banda do usuário.

e. Deve permitir a definição de quota de acesso. Tornando possível que determinados destinos (Categorias/URL/Domínio/Lista) possam ser acessados por um período limitado de tempo, e que possa ser consumido de modo não contínuo. Para exemplificação prática, queremos como resultado:
Cada usuário do grupo especificado poderá acessar o conteúdo definido na quota, em qualquer momento do dia, porém a soma de tempo deste consumo, não deverá ultrapassar o período de tempo pré-determinado para a regra.

f. Deve possuir mecanismo de classificação em tempo real dos sites visitados ou sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino. A rede de reputação não deve somente ser baseada em informações de fluxo da própria base de appliances instalados, mas sim em correlações entre outros parâmetros: Listas negras de URL, listas Brancas de URL, listas de equipamentos comprometidos, volume global de trafego, histórico dos sites, dados de categorização de URLs e web crawlers.

g. Permitir atualização automática da lista de URLs categorizadas via internet por meio de base proprietária do fabricante do equipamento.

h. Deve possuir mecanismo segurança que analise em tempo real a presença de conteúdo malicioso nas páginas acessadas.

5. ALERTAS PARA REGRAS:

a. Deve possuir mecanismo que gere alertas via e-mail quando há uma tentativa excessiva a um site bloqueado. Este alerta será disparado quando atingido o número de tentativas bloqueadas previamente pelo administrador para cada categoria.

6. MANIPULAÇÃO DE SITES:

a. Deve suportar métodos de manipulação de sites dinâmicos e sites web 2.0, ou seja, alteração de seu comportamento, de modo tal que: por exemplo:

- Redes Sociais (Facebook, Twiter, Linked-in, ...): Limitar acesso aos conteúdos ou recursos específicos dentro destes sites.
- Youtube: Limitar acesso a vídeos de determinada categoria.

7. RELATÓRIOS:

a. Deve possuir recursos que permita a partir de informações como usuário e url, o sistema possa informar se o acesso será permitido, ou negado e em que política ele passou ou o porquê foi bloqueado.

b. Deve possuir capacidade de apresentar acessos em tempo real ao log de acesso ao proxy, permitindo a filtragem por no mínimo os seguintes campos Usuário/Ip/Categoria, exibindo informações como url acessada, categoria, política utilizada no acesso ou bloqueio.

c. Deve emitir relatórios do tipo Top 10 Usuário/Categorias/Url, Top Usuários Bloqueados.

d. Deve emitir relatórios de checagem de malware, informando no mínimo as urls bloqueadas e o tipo de malware encontrado.

e. Deve exibir relatórios de atividades do usuário onde a, saibamos quais os sites/categorias acessados, bloqueados, consumo de banda este usuário acessou.

f. Deve emitir relatórios customizáveis com base a diversos critérios, produzindo documentos de múltiplos niveis.

g. Deve permitir a exportação dos dados dos relatórios para no mínimo dois dos seguintes formatos: CSV, XLS, PDF, HTML e TXT;

h. Deve possibilitar o agendamento de geração de relatório periódico, permitindo o seu envio por e-mail.

4.1 LOTE 1 – ITEM 2 – AQUISIÇÃO DE SERVIÇOS DE SUPORTE E GARANTIA

4.2.1. Aquisição de serviços de suporte e garantia, conforme especificações abaixo:

a. O proponente e o fabricante devem oferecer suporte técnico em língua portuguesa através de ligação telefônica gratuita do tipo 0800, que deve estar disponível no regime de 24 x 7 x 365 (24 horas por dia, 7 dias na semana e 365 dias no ano);

b. O hardware, software e acessórios componentes da solução devem ser fornecidos com garantia e suporte do fabricante de 12 (doze) meses, contados depois de concluídas as etapas de homologação e entrega final, com atendimento on-site, com substituição do equipamento defeituoso ocorrendo em até no máximo 07 (sete) dias úteis após a abertura do chamado ou comprovação do defeito junto ao proponente/fabricante;

c. Atualizações de firmware e correções devem estar disponíveis via Internet, sem custo adicional durante o período de garantia;

d. Em caso de falhas, fica a cargo do fornecedor o envio do produto substituto, e também é de responsabilidade do fornecedor devolver para o fabricante o produto danificado;

e. Os chamados de suporte técnico podem ser abertos com o proponente e com o suporte técnico do fabricante a critério da SEFAZ-ES;

Nível de Severidade	Descrição	E-mail	On Site
Alto	Serviço completamente indisponível		02 horas
Médio	Serviço operando parcialmente		04 horas
Baixo	Serviço com degradação de desempenho ou funcionalidade	08 horas	
Normal	Aplicação de patchs, hotfixes e firmware		Agendamento de 48 horas

f. Os chamados de severidade baixa, ou seja, aqueles que não afetam o desempenho da solução ou funcionalidades que não sejam de suma importância, devem possuir um tempo de resposta máximo de 8h (oito horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado por e-mail. Para solução do problema o SLA solicitado será apenas para hardware.

g. Os chamados de severidade média, ou seja, aqueles que influenciam negativamente no funcionamento de alguns dos seus serviços, mas sem torná-la totalmente inoperante, devem possuir um tempo de resposta máxima de 4h (quatro horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado On Site. Para solução do problema o SLA solicitado será apenas para hardware.

h. Os chamados de severidade crítica, ou seja, aqueles relacionados a impactos de alta relevância que impedem a operação da solução, devem possuir um tempo de resposta máximo de 02h (duas horas) para diagnóstico e solução do problema, o

mesmo deverá ser realizado On Site. Para solução do problema o SLA solicitado será apenas para hardware.

i. Caberá exclusivamente à SEFAZ a categorização do chamado no ato da sua abertura.

4.2 LOTE 1 – ITEM 3 – AQUISIÇÃO DE SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO PRETENDIDA

4.3.1. Aquisição de serviços de instalação e configuração da solução, conforme especificações abaixo:

- **IMPLANTAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO:**

a. A infraestrutura física e lógica do proxy hoje é composta por:

- Uma solução em cluster Fortigate (Fortinet), a qual provendo a filtragem de conteúdo por categoria e listas de URLS personalizadas;

b. Devem ser configurados na solução, todos os perfis de acesso via proxy existente na atual solução, que são compostas por 16 regras de acesso sendo:

- 1 Regra de acesso a somente um grupo de sites delimitados;
- 14 Regras de acesso para diferentes categorias de acesso à internet;
- 1 Regra de acesso durante o período de almoço (12h até 14h) a sites de Streaming com traffic shaping.

c. Deve ser configurado 5 regras permitindo acesso a ranges de IP de forma anônima para a um grupo de sites da internet.

d. Na solução atual realizamos a mudança de categoria a 130 sites localmente, caso estes sites estejam categorizados em categorias diferentes na nova solução, os mesmos devem ser reconfigurados conforme ambiente atual.

e. Deve ser configurado 65 protocolos customizados a partir de um ou um grupo de portas.

f. Devem ser levantadas junto à equipe designada SUREP (SEFAZ-ES), quais das novas funcionalidades que embora não exista na solução atual, serão implantadas durante esta migração. Esta lista terá como limite, todas as funcionalidades requeridas para o produto neste edital;

g. Deve ser proposta à equipe designada SUREP (SEFAZ-ES), as possíveis topologias (físicas e lógicas) da solução de Proxy de modo que atenda melhor a nossa necessidade diante do cenário encontrado, estando sujeito à aprovação e aceite da equipe designada da SUREP (SEFAZ-ES);

h. Antes da execução dos serviços de implantação da solução proposta, deverá ser realizada uma reunião com a presença dos arquitetos da solução do

fornecedor, os analistas da SEFAZ envolvidos no projeto e a equipe do Escritório de TI da GETEC / SEFAZ, para elaboração do plano do projeto para a implantação da solução, de forma a seguir as boas práticas de gerenciamento de projetos, incluindo:

- Estudos de viabilidade, configuração, instalação e migração;
- Detalhamento das atividades;
- Escopo;
- Cronograma;
- Recursos;
- Análise de riscos e impacto;
- Plano de contingências;
- Marcos do projeto;
- Reuniões de acompanhamento, entre outros;
- Documentação necessária.

i. Todo o processo de migração da solução para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, comprovadamente certificado e autorizado pelo fabricante do equipamento adquirido, sob a supervisão da equipe designada da SUREP (SEFAZ-ES), que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal;

j. A instalação dos equipamentos adquiridos deve ser feita de forma paralela à infraestrutura atual e a migração para o novo núcleo deve acontecer de forma programada e definida pelos analistas da SUREP (SEFAZ-ES), com o mínimo possível de interrupção do funcionamento da solução atual, devendo toda e qualquer interrupção ser comunicada, programada e autorizada pela SUREP (SEFAZ-ES);

k. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados. Os testes devem compreender a comprovação de forma inequívoca do perfeito funcionamento dos mecanismos de alta disponibilidade, sejam eles de enlace físico, switches de acesso, switches core e também seus componentes. Todos estes testes devem ser realizados com o acompanhamento da equipe de analistas da SUREP (SEFAZ-ES);

l. Documentação As-Built de todo o projeto.

m. Toda a parte de serviços de instalação e configuração devem ser executados dentro da Sefaz no formato On-site.

- **TESTE DE BANCADA**

a. Deverão ser apresentados para o pleno atendimento aos requisitos deste edital e ainda em caráter eliminatório, testes de bancada, onde deverão ser comprovadas de forma prática, todas as características e funcionalidades descritas de cada produto ou serviço deste edital. O teste de bancada devera ser executado em ambiente de Produção da SEFAZ.

b. Após a energização, instalação e configuração inicial do equipamento o fornecedor/fabricante terá um prazo de 40(quarenta) horas para demonstrar as funcionalidades solicitadas no Anexo II.

4.3 LOTE 1 – ITEM 4 – AQUISIÇÃO DE SERVIÇOS DE TREINAMENTO NA SOLUÇÃO PRETENDIDA

4.4.1. Aquisição de serviços treinamentos, conforme especificações abaixo:

- **TREINAMENTO OFICIAL DO FABRICANTE**

a. Deve ser realizado um treinamento oficial do fabricante da solução para 04 (quatro) funcionários da equipe da SUREP (SEFAZ-ES);

b. Este treinamento deverá ter no mínimo 40 horas/aula de duração, e caso este treinamento não tenha em sua ementa, todas as funcionalidades exigidas neste edital, deve ser dado um novo treinamento oficial, o qual seu conteúdo abranja as funcionalidades restantes não contempladas no primeiro treinamento.

c. O treinamento deve ser realizado em horário comercial, de segunda a sexta-feira;

d. O treinamento deverá explanar conteúdo suficiente para a plena utilização dos produtos ofertados para a solução, devendo ser um curso de currículo oficial do fabricante, mesmo que extraordinariamente complementado pela cobertura das funcionalidades específicas destes produtos, bem como as características técnicas utilizadas para o desenho de toda a solução utilizada neste projeto, incluindo técnicas de resolução de problemas;

e. Caso o conteúdo exigido não seja coberto por um único treinamento oficial, podem ser realizados tantos treinamentos oficiais quantos sejam necessários para que seja feito integralmente o repasse do conteúdo exigido, desde que obedecidos os mesmos prazos e condições estipulados neste documento;

f. O treinamento deve ser ministrado por instrutores capacitados e possuidores de certificação emitida pelo fabricante da solução, bem como a instituição que realizará o treinamento deve possuir certificação de capacitação fornecida pelo fabricante específica para execução de treinamentos;

g. Deve ser agendado a critério da SEFAZ, com antecedência de 30(trinta) dias consecutivos para o perfeito planejamento junto ao centro autorizado. Após o agendamento, o treinamento deve ser iniciado em até 60 (sessenta) dias consecutivos;

h. A SEFAZ se reserva o direito de indicar, em cada solicitação de treinamento, o número de 01 (um) até 04 (quatro) participantes, sendo que a soma de todos os participantes não ultrapassará o total de 04 (quatro);

i. O treinamento pode ser ministrado na Região da Grande Vitória ou em outras localidades:

- Os treinamentos poderão ser ministrados na Região da Grande Vitória, ou em outras localidades. Não sendo na Grande Vitória, a proposta do licitante deverá prever por sua própria conta todos os custos referentes às passagens aéreas, bem como diárias para todos os treinandos.
- Na hipótese do treinamento ocorrer fora da região metropolitana da Grande Vitória, as diárias serão pagas aos treinandos pela SEFAZ, nos valores previstos no Decreto nº 3328-R, de 17 de junho de 2013, publicado do DOES em 18 de junho de 2013, acrescido do adicional de 20% (vinte por cento) correspondente à ajuda de custo para deslocamento, conforme previsão do decreto citado. A contratada emitirá fatura pelo treinamento segundo o valor proposto na licitação, descontados os valores repassados diretamente pela SEFAZ aos treinandos a título de diária e ajuda de custo.

j. O licitante vencedor deve se responsabilizar em fornecer, sem custo adicional para a SEFAZ, local de treinamento, infraestrutura e material didático impresso na língua portuguesa (Brasil) ou língua inglesa a todos participantes para acompanhamento do treinamento;

k. Ao final de cada treinamento deve ser emitido e entregue a cada aluno certificado oficial de participação, emitido pelo próprio fabricante;

l. A entrega dos certificados oficiais de participação é condição necessária ao pagamento dos treinamentos.

- **TREINAMENTO HANDS-ON IN-LOCO**

a. Ao final dos serviços deve ser oferecido um treinamento “in loco” para repasse tecnológico de conhecimento de todo o ambiente implantado, para 06 (seis) funcionários da SUREP (SEFAZ-ES), com carga horária mínima de 16 (dezesseis) horas;

b. Deve ser conduzido por profissional, possuidor de certificação emitida pelo fabricante da solução, que detenha todas as condições técnicas (teóricas e práticas) necessárias. O responsável pelo treinamento “in loco” deve preferencialmente ser o mesmo profissional que participou das fases de elaboração de projeto e implantação da solução, e somente será aceita a sua substituição em casos excepcionais e com a concordância da SUREP (SEFAZ-ES);

c. Deve ser realizado nas dependências físicas da SEFAZ-ES entre 09h e 18h, de segunda à sexta-feira;

d. Deve contemplar a apresentação da implantação, explanando a topologia adotada e os equipamentos envolvidos;

e. Deve abordar todas as funcionalidades envolvidas no projeto da nova rede;

f. Deve capacitar os alunos a executarem tarefas rotineiras de configuração, operação, suporte, manutenção e monitoramento dos equipamentos adquiridos.

4.4 Deveres da Contratada

4.5.1 A contratada deve seguir os seguintes itens:

a. Registrar as ocorrências durante a execução do objeto, dando ciência à Secretaria da Fazenda do Estado do Espírito Santo, respondendo integralmente por sua omissão;

b. O profissional que atuará como gerente de projeto deve ter certificação como Project Management Professional (PMP);

c. Para os itens 1, 2 e 3 do lote 1 apresentar profissional(is) com certificação técnica emitida pelo fabricante ou instituto autorizado pelo respectivo fabricante do Secure Web Gateway, indicando sua habilitação técnica na tecnologia ofertada. Este profissional deve executar “in loco” os serviços especificados e prestar o suporte e o atendimento em garantia dos produtos;

d. Executar o objeto nas condições especificadas pela Secretaria da Fazenda do Estado do Espírito Santo;

e. Desenvolver os serviços sempre em regime de entendimento com a Secretaria da Fazenda do Estado do Espírito Santo;

f. Prestar os serviços sempre por intermédio do responsável legal ou por técnicos qualificados, devendo responder perante a Secretaria da Fazenda do Estado do Espírito Santo e a terceiros pela cobertura dos riscos de acidentes de trabalho de seus empregados, prepostos ou contratados, por todos os ônus, encargos, perdas e danos porventura resultantes da execução do objeto;

g. Adicionalmente, na proposta, o arrematante obrigatoriamente deverá detalhar a marca, o modelo, e a decomposição dos preços para cada parte significativa do equipamento ofertado para os Item 1 – AQUISIÇÃO DE SOLUÇÃO DE SWG – SECURE WEB GATEWAY, detalhando código (part number), descrição, unidade, quantidade, valor unitário e valor total de cada componente. A tabela a seguir exemplifica como o proponente deverá detalhar a composição dos equipamentos:

Item	Especificação	Unid.	Quant.	Valor Unitário Máximo Admitido (R$)	Valor Total Máximo Admitido (R$)
1	SWG – SECURE WEB GATEWAY (02 unidades)				
	Hardware		2		
	Software		2		
2	SUPORTE E GARANTIA				
	Hardware		36 meses		
	Software		36 meses		
3	Serviços de Instalação e Configuração				
	Hardware		1 Conjunto		
	Software		1 Conjunto		
4	Serviços de Treinamento				
	Treinamento Oficial		1 Conjunto		
	Treinamento Hands-On		1 Conjunto		

h. O arrematante também deverá detalhar em sua proposta os códigos, descrição, carga horária, quantidade de treinandos, valor unitário do treinamento por treinando e valor total.

i. Ainda, o arrematante obrigatoriamente deverá detalhar em sua proposta a composição de custos dos serviços de instalação e configuração, descrevendo o perfil de profissionais envolvidos na implementação da solução e respectivo esforço estimado em quantidade de homens x hora, o valor unitário por homem x hora e o valor total, incluindo o gerente do projeto requisitado no item i, constante nos “deveres da contratada” deste edital.

ANEXO I

MODELO DE ORÇAMENTO ESTIMATIVO

À: Secretaria de Estado da Fazenda do Espírito Santo.

Ref.: Projeto de aquisição de solução de TI – Secure Web Gateway, serviço de instalação e treinamento (Processo nº 68083068)

Prezados Senhores:

Pela presente apresentamos orçamento estimativo referente ao Projeto supracitado, com indicação do preço unitário de cada item e do preço global:

Item	Especificação	Unid.	Quant.	Valor Unitário Máximo Admitido (R$)	Valor Total Máximo Admitido (R$)
1	SWG – SECURE WEB GATEWAY (02 unidades)				
	Hardware		2		
	Software		2		
2	SUPORTE E GARANTIA				
	Hardware		36 meses		
	Software		36 meses		
3	Serviços de Instalação e Configuração				
	Hardware		1 Conjunto		
	Software		1 Conjunto		
4	Serviços de Treinamento				
	Treinamento Oficial		1 Conjunto		
	Treinamento Hands-On		1 Conjunto		

VALOR TOTAL: R$

Sem mais para o momento, firmamo-nos,
Atenciosamente,
____(Local)___,_(dia)_de_(mês)_de__(ano).

_____
Identificação e Assinatura

DADOS CADASTRAIS DA EMPRESA

Razão Social: _____
Nome Fantasia: _____
CNPJ: _____/_____/_____ - _____
Endereço: _____
Email: _____
Telefone: ( ) _____
Nome completo do responsável pelo orçamento:_____

Carimbo com Razão Social e CNPJ da Empresa

ANEXO II

Critério avaliado	Conforme	Não Conforme
Ser Appliance, mínimo 3(três) interfaces 10/100/1000BaseT, suporta montagem sobre rack 19".		
Deve prover armazenamento temporário de objetos(Cache).		
Deve forma um cluster Ativo-Ativo/Ativo-Passivo, simular queda de um dos ativos e sua reintegração no cluster.		
Deve integrar com Serviço de Diretório do Windows.		
Deve autenticar em pelo menos dois dos seguintes protocolos: Ntlm, Kerberos, ldap, radius.		
Deve ter capacidade de gerenciar com no mínimo três níveis de privilegio: Administrador, operação e emissor de relatórios.		
Deve executar todas as operações em uma console única.		
Deve possuir gerenciamento gráfico (Web) do tipo Point-and-click.		
Deve possuir auditoria de configuração.		
Deve permitir execução de copias de segurança manual e automática.		
Deve implementar os padrões de gerencia: SNMPv1, SNMPv2 e SNMPv3, incluindo traps.		
Deve permitir a criação de regra permitindo ou bloqueando por aplicações.		
Deve suportar HTTP, HTTPS e FTP.		
Deve permitir a criação de regra de acesso permitindo ou bloqueando pelos seguintes critérios: Origem, destino, tipo de arquivo, protocolo e horário.		
Deve Permitir controlar a quantidade de largura de banda utilizada para determinadas Categoria.		
Deve permitir a definição de quota de acesso.		
Deve possuir mecanismo de classificação em tempo real dos sites visitados.		
Deve possuir mecanismo segurança que analise em tempo real a presença de conteúdo malicioso nas páginas acessadas.		
Deve possuir mecanismo que gere uma alerta via e-mail acusando quando há uma tentativa excessiva a sites bloqueados.		
Deve suportar métodos de manipulação de sites dinâmicos e sites web 2.0.		
Deve possuir capacidade de apresentar acessos em tempo real ao log de acesso ao proxy.		
Deve emitir relatórios do tipo Top 10 Usuários/Categorias/url, Top Usuários Bloqueados.		
Deve emitir relatórios de checagem de malware, informando no mínimo as urls bloqueadas e o tipo de malware encontrado.		
Deve exibir relatórios de atividades do usuário os sites/categorias acessados, bloqueados, consumo de banda este usuário acessou.		
Deve permitir a exportação dos dados dos relatórios para no mínimo dois dos seguintes formatos: CSV, XLS, PDF, HTML e TXT		
Deve possibilitar o agendamento de geração de relatório periódico, permitindo o seu armazenamento em caminho externo via compartilhamento.		
Deve possuir recursos que permita a partir de informações como usuário e url,		
Deve por meio de informação como usuário e url informar se o acesso foi bloqueado ou permitido e em qual regra o acesso passou.		