



CONSULTA PÚBLICA Nº 003/2015

A Secretaria de Estado da Fazenda - SEFAZ realizará oportunamente processo de licitação visando à aquisição de solução de TI – *Application Delivery Controller*, serviço de instalação e treinamento, no âmbito do Plano de Desenvolvimento da Administração Fazendária – PROFAS 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 15/09/2015 a 01/10/2015**, 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 – *Application Delivery Controller*

1.2 OBJETIVO

Tem por finalidade a aquisição, o gerenciamento e a manutenção da ferramenta que garante disponibilidade e o funcionamento balanceado dos sites e promove a segurança dos sistemas disponibilizados através dos sites desta secretaria.

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 não deve ser inferior a 36 (trinta e seis) meses, contados a partir da data de homologação do projeto na secretaria.

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, pelas gerências:

- GETEC – Gerência de Tecnologia da Informática
- SUINT – Subgerência de Infraestrutura Tecnológica



PARTE 2 – CONTEXTUALIZAÇÃO

2.1 BENEFÍCIOS DOS PRODUTOS

O produto em questão viabilizará o acesso aos sites desta secretaria, garantindo maior disponibilidade e balanceamento. Promoverá maior segurança aos sistemas disponibilizados através dos sites desta secretaria.

PARTE 3 – OBJETIVO GERAL DO PROJETO

3.1 JUSTIFICATIVA

A aquisição de uma solução moderna para atendimento desta necessidade vem se tornando cada vez mais eminente, pois é sabido que uma solução de “Application Delivery Controller” além de prover disponibilidade e balanceamento, também tem como responsabilidade garantir maior segurança aos sistemas disponíveis na internet, através dos sites desta secretaria.

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

Para atender a esta demanda a secretaria conta com um produto antigo, que não realiza todas as funcionalidades hoje necessárias para disponibilidade segura de um sistema na internet. O produto que utilizamos hoje, não possui licença e contrato. Em razão disso, a aquisição trará além da solução técnica através do atendimento das necessidades de segurança e disponibilidade, também uma gerência centralizada, e compreendida, permitindo assim o controle sobre as informações contidas nos sistemas disponibilizados nos sites desta secretaria.

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 quando aplicável.

Aquisição de solução de TI para as unidades da SEFAZ, solução de ADC – *Application Delivery Controller*, conforme a seguir.



4.1 LOTE 1 – ITEM 1 – AQUISIÇÃO DE SOLUÇÃO DE ADC – APPLICATION DELIVERY CONTROLLER

4.1.1. Aquisição de solução ADC – Application Delivery Controller, conforme especificações técnicas abaixo:

4.1.2. QUANTIDADE: 2(dois).

4.1.3. PRAZO DE ENTREGA: EM ATÉ 30 DIAS APÓS A ASSINATURA DO CONTRATO.

4.1.4. CONFORME ESPECIFICAÇÕES:

- a. O equipamento deve ser composto por 02 (dois) appliances em alta-disponibilidade, cada um dotado de 6 (seis) portas 10/100/1000Mbps BaseT e 2 (duas) portas 10Gbps SFP;
- b. Devem ser fornecidos hardware, software e licenças em quantidade suficiente para atender todos os requisitos listados nesta aquisição;
- c. Os equipamentos deverão ser novos, sem uso, e serem produzidos em série na época da entrega;
- d. Os hardwares e softwares ofertados na composição deste item não devem estar listados como “End Of Sale” e “End Of Life” por seus respectivos fabricantes até a data da abertura das propostas.
- e. Os Appliances ofertados pela CONTRATADA para o atendimento dos requisitos de todo o edital devem ser do mesmo fabricante, de forma a maximizar sua compatibilidade e funcionalidade.

4.1.5. Especificações Físicas e de Desempenho:

- a. Deverá ser fornecido em equipamento do tipo appliance, ou seja, módulo projetado especificamente para atender a solução, com sistema operacional otimizado para esse fim e instalável em rack padrão 19”.
- b. Possuir quantidade de memória e processamento mínima suficiente para atendimento de todas as funcionalidades e o desempenho solicitados neste documento.
- c. Deve possuir uma porta de gerenciamento out-of-band de, no mínimo, 10/100/1000Mbps. A porta de gerência deve ser fisicamente isolada das portas de tráfego, não sendo aceitas portas comuns às duas funções.
- d. Deve possuir, pelo menos, 1 porta serial (RS232 ou RJ45) ou USB para gerenciamento.
- e. Deve possuir LEDs indicadores de status, atividade de rede, status dos links e alimentação.
- f. Deve possuir fonte de alimentação 110/220 v (AC).
- g. Devem ser fornecidas duas fontes de alimentação instaladas em cada equipamento para maior redundância.



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

- h. A alimentação será disponibilizada em dois circuitos. O equipamento deverá manter a operacionalidade em caso de falha em qualquer um deles.
- i. O plugue deve ser padrão ABNT NBR 14136 ou NEMA 5-15 com adaptador para ABNT NBR 14136. Caso seja necessária a substituição, deve ser realizada pela CONTRATADA sem prejuízo de garantia e suporte.
- j. Devem ser fornecidos todos os GBICs e SFPs necessários para o atendimento de todos os itens deste EDITAL.
- k. Suportar no mínimo 5 Gbps de tráfego de Camada 7 por appliance;
- l. Suportar no mínimo 375 mil requests por segundo de Camada 7;
- m. Suportar no mínimo 5 milhões de conexões concorrentes de Camada 4;
- n. Suportar no mínimo 20 mil Transações por Segundo de SSL com certificados de 1024 bits;
- o. Suportar no mínimo 4 mil Transações por Segundo de SSL com certificados de 2048 bits;
- p. Suportar, no mínimo, 4 Gbps de tráfego SSL;
- q. Deverá possuir throughput mínimo de 2 Gbps para compressão HTTP;
- r. Mecanismo de redundância de dispositivos em modo ativo-ativo e ativo-passivo, de forma que em caso de falha de um dos equipamentos o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência.
- s. Implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades.
- t. A solução deve possuir suporte ao espelhamento de conexões HTTP entre o appliance ativo e standby.
- u. Agregação de portas baseado no protocolo LACP(IEEE 802.3ad).
- v. Transporte de múltiplas VLANs por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q.
- w. Spanning-Tree (IEEE 802.1D) e Fast Spanning-Tree (IEEE 802.1w, IEEE 802.1t).
- x. Deve possuir capacidade de armazenamento de logs do sistema, para identificação de funcionamento dos principais componentes de gerenciamento e armazenar logs de auditoria, para registro de todas as atividades dos usuários da ferramenta.
- y. Balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.
- z. Implementar as seguintes funcionalidades de segurança:
 - i. Network Address Translation (NAT);
 - ii. Proteção contra SynFlood;
 - iii. Limite do número de conexões;



iv. Listas de Controle de Acesso (ACL);

- aa. A solução deve implementar capacidade de virtualização de equipamentos, permitindo que um único chassi possa ser “particionado” em múltiplos appliances virtuais que serão configurados e gerenciados de forma isolada.
- bb. A Solução deve ser entregue com todos os recursos necessários para criar até 04 (quatro) contextos virtuais por Appliance.
- cc. Os contextos poderão compartilhar os recursos de hardware entre si.
- dd. Suporta a inspeção, balanceamento, filtragem e bloqueio de tráfego com base no User-Agent localizado no cabeçalho HTTP.
- ee. Ao modificar a política de segurança, os itens presentes no Cache da solução e utilizados para otimização e aceleração das aplicações devem refletir as novas políticas. A limpeza do cache afetado pela mudança na configuração do equipamento deverá ser automaticamente executada ou deve ser possível, através da interface de gerência, executar manualmente a limpeza do cache da(s) aplicação(ões) afetada(s).
- ff. Deve possuir suporte a endereçamento IPv6.

4.1.6. Balanceamento de servidores:

- a. a. Possuir algoritmo de balanceamento de carga de servidores no mínimo baseado nos métodos Round-Robin, menor número de conexões (least connections), atribuição de pesos diferentes, baseado em endereços IP de origem e destino, URL e tempo de resposta
- b. Possibilita limitar o número de sessões estabelecidas com cada servidor real, com a possibilidade de redirecionar as conexões excedentes a um portal personalizado com uma “resposta amigável” ao usuário.

4.1.7. Persistência

- a. A solução deve, além de balancear as sessões novas, preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
 - i. Por cookie;
 - ii. Por endereço IP destino;
 - iii. Por Endereço IP origem;
 - iv. Por sessão SSL;
 - v. Analisando a URL acessada;
 - vi. Analisando qualquer parâmetro no header HTTP;

4.1.8. Monitoramento de Servidores – Health Check

- a. A solução deve implementar os seguintes métodos de monitoramento dos servidores reais, de forma nativa ou através do uso de monitores personalizados:
 - i. Camada 3 – ICMP;



- ii. Camada 4 – Conexões TCP e UDP pela porta respectiva no servidor;
- iii. Camada 7 – Conexões específicas ao protocolo de aplicação, suportando, no mínimo: HTTP, HTTPS, FTP, SMTP, LDAP, IMAP, POP3, SIP e SNMP;

4.1.9. Otimização de tráfego

- a. A solução deve permitir o gerenciamento de banda e priorização de tráfego de entrada para determinadas aplicações.
- b. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede ou priorização de tráfego com foco na aplicação.
- c. A solução deve realizar Controle de Banda Dinâmico para grupos de aplicações e rede ou priorização de tráfego com foco na aplicação.
- d. A solução deve realizar Controle de Banda baseado em domínio de roteamento ou priorização de tráfego.
- e. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes.
- f. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação;
- g. A solução deverá ser capaz de abrir um número específico de conexões TCP com o servidor web e inserir todos os HTTP requests gerados pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço.
- h. Permitir a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor.
- i. Deverá ser capaz de fazer compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente:
 - i. Deve permitir compressão tipo GZIP e Deflate;
 - ii. Deve ser possível definir compressão por tipo de objeto analisado;
- j. A compressão deve ser feita em hardware dedicado para não afetar a performance do appliance.
- k. Implementar Cache de Conteúdo para HTTP, permitindo que objetos sejam armazenados em RAM e requisições HTTP sejam respondidas diretamente pela solução:
 - i. O recurso de cache deverá permitir a definição de quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados;
 - ii. O recurso de cache deve permitir o ajuste de quanta memória será utilizada para armazenar objetos;

4.1.10. SSL Offload



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

- a. Deverá ser capaz de fazer (OffLoad) de SSL/TLS, onde os certificados digitais são instalados na solução ofertada e todos os itens abaixo são plenamente atendidos:
 - i. Na aceleração de SSL/TLS, no mínimo as operações de troca de chaves e criptografia dos dados devem ser feitas com aceleração em hardware, de forma a não onerar o desempenho sistema;
 - ii. Deve ser possível configurar a solução de forma que as requisições HTTP sejam enviadas aos servidores sem criptografia;
 - iii. Deve ser possível configurar a solução de forma que o tráfego SSL/TLS seja re-criptografado antes de enviá-lo ao servidor real, permitindo as demais otimizações em ambiente 100% criptografado;
 - iv. Ao re-criptografar em SSL/TLS a requisição antes de enviá-la ao servidor, deve ser possível configurar um algoritmo e tamanho de chave distinto ao utilizado no estabelecimento do túnel criptografado entre o cliente e o ADC;
- b. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
 - i. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS;
 - ii. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS;
 - iii. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
- c. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:
 - i. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;
 - ii. Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;
- d. A validação de certificados digitais utilizados pelo cliente para autenticar-se a serviços onde o túnel SSL é fechado entre o cliente e o ADC deve atender aos itens a seguir.

O atendimento dos itens abaixo não é obrigatório caso a solução implemente funcionalidade onde o túnel SSL seja fechado entre o cliente e servidor real e nesta configuração todas as capacidades de segurança, balanceamento e otimização solicitadas no EDITAL sejam mantidas sem restrições:



- i. Deverá ser feita via Cadeia de ACs Confiáveis configurada pela SEFAZ-ES;
- ii. A solução deve, mediante configuração, verificar a validade do Certificado Digital apresentado pelo cliente através de CRL – Lista de Certificados Revogados;
- iii. Deve ser possível configurar um período de cache para a CRL de forma que dentro do tempo configurado o equipamento não consulte novamente a Lista de Certificados Revogados, utilizando neste caso a cópia em Cache;

4.1.11. Log

- a. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:
 - i. Endereço IP de origem;
 - ii. Porta TCP ou UDP de origem;
 - iii. Endereço IP de destino;
 - iv. Porta TCP ou UDP de destino;
 - v. Protocolo de camada 4 (TCP ou UDP);
 - vi. Data e hora da mensagem;
 - vii. URL acessada;
- b. A solução deve ser capaz de analisar a performance de aplicações web.
- c. A solução deve possuir relatórios das aplicações.
- d. Deve prover métricas de aplicações como: Transações por segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões.

4.1.12. Funcionalidades de Gerenciamento da Solução

- a. Deve suportar interface de gerenciamento baseado em protocolo HTTP seguro (HTTPS), acessível por navegador de Internet como MS Internet Explorer, Chrome, entre outros.
- b. Suporta controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.
- c. Suporta criação de ACL (Access Control List – Lista de Controle de Acesso), especificando quais endereços IP terão permissão de comunicação com a gerência.
- d. Em toda e qualquer situação de gerenciamento remoto, a comunicação entre o sensor e o sistema de gerenciamento central deverá ser criptografada através dos mecanismos SSL ou SSH.
- e. Deve permitir que sejam configurados pelo menos 03 (três) perfis de acesso ao equipamento:
 - i. Operador: Acesso básico para visualização do sistema;



- ii. Administrador de Aplicações: Acesso avançado para monitorar e gerenciar as configurações de uma aplicação balanceada através do equipamento, permitindo adicionar e remover servidores reais ao Pool, ativar e desativar o serviço;
- iii. Super Usuário: Acesso completo para monitorar e gerenciar todas as funções do sistema;
- f. Suporta autenticação de usuários e administradores através:
 - i. Autenticação local: usuários e administradores cadastrados na gerência;
 - ii. Autenticação LDAP: usuários e administradores importados/integrados com o Windows AD (Active Directory);
 - iii. Autenticação RADIUS: usuários e administradores importados/integrados com servidor RADIUS;
- g. Deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.
- h. Deve ser capaz de realizar notificações de eventos de segurança através de e-mail, traps SNMP e Syslog.
- i. Deve possuir capacidade de armazenamento de logs de auditoria, para registro de todas as atividades dos usuários da ferramenta.

4.1.13. Segurança

- a. A solução deverá identificar, isolar e bloquear ataques sofisticados, sem impactar nas transações das aplicações e nas funções de balanceamento de cargas e otimização de tráfego.
- b. Permitir que apenas transações de aplicações validadas sejam aceitas, o restante das transações deve ser bloqueado.
- c. A solução deverá implementar as seguintes funcionalidades de segurança:
 - i. Web Application Firewall integrado – conforme funcionalidades descritas neste projeto;
 - ii. Firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação;
 - iii. Permitir a utilização de um modelo positivo de segurança para proteger contra-ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes;
 - iv. Possuir política de segurança de aplicações web pré-configurada na solução;
 - v. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes;



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

- vi. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies;
- d. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do equipamento. O resultado desta análise deve ser utilizado para configurar as políticas do mesmo.
- e. A solução deverá possuir funcionalidade de proteção positiva e segura contra ataques, como:
 - i. Manipulação de entradas inválidas – Ataques de Injeção;
 - ii. Controle de Acesso Bruto (Ataque bruto via browser);
 - iii. Buffer Overflow;
 - iv. Cross-Site Script;
 - v. SQL/SO Injection;
 - vi. Cookie poisoning;
 - vii. HTTP Request Smuggling;
 - viii. Manipulação de campos escondidos;
 - ix. Manipulação de cookies;
 - x. Roubo de sessão através de manipulação de cookies;
- f. Possui mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML.
- g. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;
- h. Deverá balancear os tráfegos de FTP e SMTP entre os servidores;
- i. É capaz de identificar e bloquear ataques através de:
 - i. Assinaturas, com atualização periódica da base pelo fabricante;
 - ii. Perfis de utilização;
- j. Detecta ataques de força bruta e Negação de Serviço:
 - i. Quantidade de transações por segundo (TPS), monitorando a quantidade de transações por segundo por endereço IP;
 - ii. O atacante solicita repetidamente o mesmo recurso;
 - iii. O atacante realiza repetidas tentativas não autorizadas de acesso;
 - iv. São utilizados ataques automatizados de login;
- k. Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:
 - i. Sistema operacional e servidor web com impressão digital;



- ii. Esconder qualquer mensagem de erro HTTP dos usuários;
- iii. Remover as mensagens de erro às páginas que serão enviadas aos usuários;
- l. Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.
- m. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro X-forwarded-for (XFF).

4.2 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 36 (trinta e seis) 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 patches, 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.

4.3 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. Todo o processo de migração será precedido de um estudo e entendimento da atual infraestrutura em funcionamento hoje na SEFAZ, englobando sua topologia, as configurações em uso;
 - b. A infraestrutura física e lógica de balanceamento hoje é composta por:
 - Um Foudry ServerIron, que executa a função de balanceado de carga;
 - c. Devem ser configurados na solução todas as configurações já existentes:
 - i. 34 Hosts Físicos;
 - ii. 18 Hosts Virtuais;
 - iii. 4 Protocolos;
 - d. Devem ser configurados na solução, as funções de aceleração de aplicação e de firewall de aplicação.
 - e. 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;
 - f. 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);



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

- g. 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.
- h. 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;
- i. 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);
- j. 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);
- k. Documentação As-Built de todo o projeto.
- l. 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 deverá 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 1.

4.4 - 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



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

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.

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 APPLICATION DELIVERY CONTROLLER, 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;



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

- 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 ADC – APPLICATION DELIVERY CONTROLLER, 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 – APPLICATION DELIVERY CONTROLLER (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.



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

ANEXO I

MODELO DE ORÇAMENTO ESTIMATIVO

À: Secretaria de Estado da Fazenda do Espírito Santo.

Ref.: Projeto de aquisição de solução de ITEM 1 – AQUISIÇÃO DE SOLUÇÃO DE ADC – APPLICATION DELIVERY CONTROLLER, serviço de instalação e treinamento (Processo nº 70877696)

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 – APPLICATION DELIVERY CONTROLLER (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



GOVERNO DO ESTADO DO ESPÍRITO SANTO
SECRETARIA DE ESTADO DA FAZENDA

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