ANEXO I

ESPECIFICAÇÕES TÉCNICAS

ESPECIFICAÇÕES TÉCNICAS

1 OBJETO

Atualização de licenciamento e fornecimento de appliances firewall Checkpoint, incluindo os serviços de implantação, suporte técnico, manutenção e garantia por 36 meses.

1.1 Descrição e Entrega

1.1.1 Atualização de licenciamento e aquisição de *hardware*, tipo *Appliance Checkpoint Next Generation Firewall*, acessórios, garantia, licenças de *software*, *softwares* de gerenciamento e manutenção, serviço de instalação, configuração, migração e suporte técnico remoto e local.

1.1.2 Todos os equipamentos físicos contidos nesta especificação técnica deverão ser entregues na ITAIPU, no endereço:

Av. Tancredo Neves, 6731 - Usina Hidrelétrica de Itaipu
Superintendência de Informática – SI.GG
Foz do Iguaçu - Paraná - Brasil

2 LICENCIAMENTO

2.1 As licenças deverão ser fornecidas conforme a tabela abaixo, e deverão dar o direito à ITAIPU de atualizá-las durante a vigência do contrato:

ITEM	DESCRIÇÃO	PART-NUMBERS	QUANT.
1	5900 Next Generation Threat Prevention & SandBlast (NGTX) Appliance - High Performance Package 32Gb Memory	CPAP-SG-59XX-INV-HPP (HW) CPAC-RAM16GB-5900-INSTALL (HW)	2
2	Aquisição Licenças Firewall, VPN, Identity Awarness, IPS, Anti-bot, Anti Virus, Anti Spam, Threat Emulation e Threat Extration	CPSB-NGTX-5900-1Y (SW) CPSB-NGTX-5900-1Y-HA (SW)	2
3	Licenças e assinaturas Check Point	CPCES-CO-STANDARD-ONSITE-12M CPCES-CO-STANDARD-12M (Renovação): CPSB-EVNT-C1000 CPSB-RPRT-N-C1000 CPSB-MOB-200 CPSB-MOB-200-HA CPSM-P1003 CPSM-C1000	3
4	Licença de Fireflow com recurso de Active Change para 1 cluster de Firewall	AFF-CL-SSP-1Y (SW) AFFAC-CL-SSP-1Y (SW)	1
5	Algosec Licença FireFlow com Active Change	AFFAC-CL-SSP-1Y (SW)	2
6	Renovação Licença Firewall Analyser para 1 cluster de Firewall Check Point	AFA-CL-SSP-1Y (SW)	3

	com Suporte 12 meses		

2.2.1 Define-se direito de atualização de versão como direito estendido por 36 meses, para atualização dos softwares, incluindo versões maiores (*major releases*), versões menores (*minor releases*), versões de manutenção (maintenance releases) e atualizações de qualquer natureza (*updates* e *patches*) que forem disponibilizadas para todos os *softwares* especificados acima, tradicionalmente disponibilizadas por meio de *download* a partir da página *web* do fabricante, sem ônus adicionais.

2.2.2 Ao identificar uma vulnerabilidade de segurança, a CONTRATADA envidará os maiores esforços para que o fabricante realize as correções no menor tempo possível.

3 HARDWARE - APPLIANCES

3.1 Entregar 2 unidades de a*ppliance* para *gateways* de segurança, com as seguintes características: *Stateful Inspection Firewall*, Identificação de usuários para aplicação de regras de acesso, VPNs (ipsec e mobile access), Controle de aplicações, Filtro de Urls, IPS, Antivirus, Anti-bot, Controle de ameaças desconhecidas (*Sandbox*) e Inspeção de tráfego SSL.

3.2 Cada unidade deverá suportar:

a) Desempenho requerido de Prevenção de Ameaças Throughput 6,75 (Gbps);
b) Desempenho requerido de Firewall Throughput 52 (Gbps);
c) Desempenho requerido de VPN de 10.2 (Gbps);
d) Deverá suportar 3.200.000 conexões simultâneas;
e) Deverá suportar 185.000 novas conexões por segundo;
f) Deverá possuir um visor gráfico LCD na parte da frente do equipamento;
g) Deverá possuir no mínimo 1 (uma) interface exclusiva para sincronismo 10/100/1000Base-T RJ45;
h) Deverá possuir no mínimo 1 (uma) interface exclusiva para gerenciamento 10/100/1000Base-T RJ45;
i) Deverá possuir módulo de expansão de pelo menos 4 (quatro) interfaces 10 Gbase-F SFP+ com os transceivers;
j) Deverá possuir pelo menos 8 (oito) interfaces 10/100/1000Base-T RJ-45;
k) Deverá possuir no mínimo 1 (uma) interface console RJ-45 e 1 (uma) micro USB;
l) Deverá possuir 1 (um) disco de no mínimo 500GB (HDD) ou 1 (um) SSD de 240GB;
m) O appliance deve possuir porta LOM (Light Out Management);
n) Caso o appliance ofertado possua interfaces além da quantidade solicitada dos modelos SFP, SFP+ e CFP2 ou qualquer outro modelo, deverão ser fornecidos todos os transceivers/transceptores necessários e licenças para a plena utilização;
o) O appliance deve suportar futura adição/troca de interfaces por um módulo de bypass físico (fail-open) com 4 (quatro) interfaces 10/100/1000Base-T ou 2 (duas) interfaces 10 GE Fibra;
p) Deverá possuir no mínimo 2 (duas) interfaces USB 3.0;
q) Deverá suportar os protocolos de roteamento OSPFv2 e v3, BGP e RIP;
r) Deverá suportar Policy-based routing;
s) Deverá suportar PIM-SM, PIM-SSM, PIM-DM, IGMP v2 e v3;
t) Possuir 2 (duas) fontes redundantes de alimentação internas bivolt 100~240V Hot Swappable.

4 CARACTERÍSTICAS GERAIS DA PLATAFORMA

4.1 A plataforma de segurança que gerencia os aplliances da seção anterior, deve conter as seguintes funcionalidades:

a) Por funcionalidades de NGTP - Next Generation Threat prevention, entende-se: reconhecimento e controle granular de aplicações web 2.0, prevenção de ameaças, identificação de usuários, IPS e Firewall;
b) As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;
c) A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
d) O software deverá ser fornecido em sua versão mais atualizada, não sendo permitido qualquer tipo de comprovação futura;
e) Todas as funcionalidades descritas no subitem 1.1, no caso NGTP, devem funcionar no mesmo appliance ou servidor virtual sem a necessidade de composição de um ou mais produtos;
f) Todo o ambiente deverá ser gerenciado através de uma única interface sem a necessidade de produtos de terceiros para compor a solução;
g) Tanto os Gateways de Segurança bem como a gerência centralizada deverão suportar monitoramento através de SNMP v1, v2 e v3;
h) O Gateway de Segurança deve ser capaz de suportar as seguintes funcionalidades gerenciamento unificado de aplicações em uma única plataforma;
i) Stateful Inspection Firewall;
j) Intrusion Prevention System (IPS);
k) Identificação de Usuários;
l) Controle de Aplicações;
m) Filtro URL;
n) AntiBot e AntiVirus;
o) Controle de ameaças desconhecidas (Sandboxing);
p) AntiSpam and Email Security;
q) IPSec VPN;
r) Mobile Access
s) Security Policy Management;
t) Logging & Status;
u) Correlação de Eventos e Relatórios;
v) A solução deverá prover mecanismo que constantemente educa o usuário final das políticas de segurança em tempo real.

5 SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E MIGRAÇÃO

5.1 A CONTRATADA deverá fornecer serviço de instalação, configuração de todos os itens adquiridos, além da migração da atual solução de firewall para a nova plataforma. Esses serviços compreendem:

a) Elaboração de um plano de trabalho e cronograma tentativo para as atividades a serem realizadas, em até 30 dias corridos após a OIS (Ordem de Início dos Serviços);

b) Instalação e/ou atualização para última versão disponível dos softwares detalhados no subitem 2.2, em até 45 dias corridos após a OIS;

c) Integrar os elementos da solução aos produtos de monitoramento usados por ITAIPU, como Tivoli Monitoring e Control Desk, Splunk e AlgoSec, preferencialmente através de chamadas REST/SOAP, ou intercâmbio de arquivos CSV;

d) Migração do ambiente atual com aplicação de regras otimizadas, podendo ser utilizado o Firewall Analyser Algosec, já licenciado por ITAIPU;

e) Validação da solução e funcionalidades conforme Plano de Trabalho;

f) Elaborar documentação detalhada da nova infraestrutura;

g) Elaboração de relatório técnico dos trabalhos realizados e resultados obtidos, em até 20 dias após a conclusão dos trabalhos de instalação previstos no subitem 5.1.

6 SUPORTE TÉCNICO

O Suporte técnico será realizado pela CONTRATADA (podendo ser prestado com apoio da FABRICANTE), sob demanda da ITAIPU, visando a operação continuada da solução. Para tal, deve observar:

a) A CONTRATADA se compromete a não divulgar dados ou informações relacionados aos produtos objeto destas especificações, mantendo sigilo absoluto em relação a todos os dados acessados ou que venham a ser gerados, no processo de prestação dos serviços (conforme termo de confidencialidade);

b) Mensalmente a CONTRATADA, deverá enviar um relatório consolidado de suporte, contendo:
1. Total de chamados remotos realizados no mês;
2. Total de visitas locais realizadas no mês (incluindo o total de horas consumidas do banco de horas, bem como saldo restante);
3. Relatório dos chamados e visitas realizados.

6.1 Suporte Técnico Remoto

6.1.1 As chamadas de suporte técnico (remoto e local) deverão ser realizadas por meio de um número telefônico, por e-mail e outras vias indicadas pela CONTRATADA, sendo de sua responsabilidade a disponibilidade do atendimento durante a vigência do contrato, e a imediata confirmação da abertura do chamado pela ITAIPU.

6.1.2 O suporte técnico remoto é um serviço que deve complementar e agilizar a solução de problemas e deve estar disponível no modelo de 24x7 (ou seja, 24 horas por dia, 7 dias por semana) durante a vigência do contrato.

6.1.3 O encerramento do atendimento deve ser atestado pela ITAIPU.

6.1.4 O não cumprimento, pela CONTRATADA, dos prazos estabelecidos implicará nas penalidades previstas em contrato.

6.1.5 O nível de criticidade do evento será definido pela ITAIPU, que informará a CONTRATADA quando da formalização do chamado.

6.1.6 A CONTRATADA deverá informar os canais de comunicação para abertura de chamados de suporte, bem como os mecanismos de registro e acompanhamento das ocorrências visando o controle dos SLA s definidos acima.

6.1.7 Nível de serviço a ser cumprido, conforme a Tabela a seguir:

SEVERIDADE	DESCRIÇÃO	INICIO DE ATENDIMENTO	FINALIZAÇÃO DO ATENDIMENTO
0	Crítico	30 min	4 h
1	Agudo	2 h	8 h
2	Normal	4 h	16 h
3	Consulta	8 h	48 h

1. A ITAIPU definirá o nível do chamado quando da sua abertura, de acordo com o impacto em seu ambiente. Os tempos são contados a partir da efetivação do chamado junto a CONTRATADA pela ITAIPU, e só serão considerados terminados quando da aceitação da solução do referido chamado pela ITAIPU (conforme subitem 6.1.3).

2. O início da prestação do serviço de suporte técnico remoto, que poderá ser feito mediante soluções de acesso remoto como VPN, Citrix, WEBEX ou de solução da própria CONTRATADA, não poderá ultrapassar o tempo máximo estabelecido na coluna PRAZO PARA INICIO DO ATENDIMENTO, a partir da abertura do chamado pela ITAIPU, tendo a CONTRATADA até o tempo máximo estabelecido na coluna PRAZO PARA CONCLUSÃO DO CHAMADO para concluir as ações de suporte para efetiva solução do problema ou solução de contorno.

6.1.8 A CONTRATADA deverá disponibilizar o endereço de extranet (URL) do sistema de Service Desk para registro da ocorrência, data, horário, severidade e acompanhamento dos chamados, além de dois números de telefone e dois endereços eletrônicos (e-mail), para os chamados da ITAIPU.

6.1.9 Nas opções de contingência de atendimento, a data e o horário de abertura do chamado serão os de envio do e-mail pela ITAIPU, transmissão do fax, ou término do contato telefônico.

6.1.10 Para cada manutenção a CONTRATADA deverá emitir relatório técnico detalhado com foco resolução técnica do evento, visando o reestabelecimento normal do ambiente. Este relatório será apresentado junto com relatório mensal com as ocorrências.

6.1.11 Considera-se plenamente solucionado o problema quando restabelecidos os sistemas ou serviços sem restrições, ou seja, quando não se tratar de uma solução paliativa.

6.2 Suporte Técnico Local

6.2.1 As horas previstas para suporte técnico local no regime de banco de horas podem ser utilizadas em qualquer quantidade e período, dependendo da demanda da ITAIPU, ao total máximo de 720 horas, durante a vigência da contratação, com previsão de uso de 240h por ano.

6.2.2 Apenas serão faturadas horas do banco efetivamente utilizadas, devendo ser previamente solicitadas, agendadas e aprovadas pela ITAIPU. Estas devem obedecer ao seguinte critério de equivalência para consumo (em horas):

TIPO DE SERVIÇO	UNIDADE	QUANTIDADE	EQUIVALÊNCIA
Suporte on-site (horário comercial)	h	1	1

Suporte on-site (noturno)	h	1	1.5
Suporte on-site (finais de semana e feriados)	h	1	2

Tabela 2: Tipo de serviço e consumo

6.2.3 Somente deverão fazer parte do cômputo das horas consumidas as atividades desenvolvidas *on-site* nos escritórios designados pela ITAIPU ou em local previamente aprovado pela área gestora. Não deverão fazer parte deste cálculo as horas consumidas desde o deslocamento do técnico até a sua apresentação na ITAIPU.

6.2.4 A CONTRATADA deverá prestar serviço de suporte técnico local, conforme demanda programada ou planejamento prévio, na modalidade de banco de horas, no total de 720 horas a serem realizadas, conforme critério de ITAIPU, na Usina Hidrelétrica de ITAIPU (Foz do Iguaçu - PR) ou no Colocation de ITAIPU no Datacenter da Primesys (Bairro da Lapa, São Paulo, capital).

6.2.5 Qualquer atuação dos técnicos alocados pela CONTRATADA, para atendimento ao suporte técnico local, deverá ser previamente solicitada pela ITAIPU através de documento e/ou canais de comunicação especificados quando do inicio dos trabalhos.

6.2.6 Durante os serviços de suporte, os consultores não poderão atender a chamados de suporte técnico oriundos de fontes diferentes das explicitamente especificadas pela ITAIPU.

6.2.7 Entre os serviços de suporte técnico estão compreendidos, não limitados a:

a) Realizar, conforme demanda de ITAIPU, atualizações de software e firmware, que envolvam produtos deste contrato;

b) Elaborar relatórios de segurança e conformidade;

c) Realizar análise de regras, e eventos de segurança;

d) Apoiar a elaboração e a implementação de planos de otimização de regras de firewall, IPSs, WAF e configuração de outros elementos da infraestrutura de segurança;

e) Propor e apoiar a implementação das melhores práticas de mercado em infraestrutura de segurança;

f) Realizar análise e testes de segurança de acordo com a demanda e em comum acordo com ITAIPU;

g) Suporte aos planos de melhoria e prospecção tecnológica na infraestrutura de segurança da ITAIPU;

h) Apoiar na definição e implementação de mecanismos de monitoramento de segurança;

i) Orientar quanto a procedimentos de auditoria forense e correlacionamento de eventos no ambiente de segurança relacionados aos equipamentos objeto desse contrato;

j) Apoiar a integração da solução ofertada com soluções de monitoramento existentes

em ITAIPU.

6.2.8 Para as atividades solicitadas de apoio de suporte técnico local, deverá ser entregue um relatório detalhando contendo as informações conclusivas do esforço realizado, conforme item 6, letra b).

7 QUALIFICAÇÃO TÉCNICA DOS PROFISSIONAIS

7.1 Para execução dos serviços de instalação, configuração, migração e suporte técnico local, a CONTRATADA deverá alocar profissionais cujas certificações contemplem pelo menos as relacionadas abaixo. Os certificados devem ser emitidos pelas entidades certificadoras correspondentes.

a) CCSE – Checkpoint Certified Security Expert;

b) CISSP – Certified Information Systems Security Profesional ou CISM - Certified Information Security Manager.

7.2 A CONTRATADA deverá possuir profissionais com experiência de implantação do produto AlgoSec e disponibilizar para as atividades técnicas, profissionais com as certificações exigidas nas letras a) e b) do subitem 7.1.

7.3 A CONTRATADA deverá apresentar em até 30 dias corridos a partir da Ordem de Início de Serviços, os documentos comprobatórios das certificações exigidas no subitem 7.1.

7.4 A substituição dos profissionais só poderá ser realizada após consulta, comprovação de certificação e respectiva aprovação pela ITAIPU.

8 GARANTIA

8.1 A CONTRATADA deverá fornecer serviço de manutenção e substituição de hardware, caso necessário, em até 2 (dois) dias úteis após aprovação do fabricante à solicitação de troca do equipamento e/ou partes (processo de RMA), em caso de falha ou defeito nos equipamentos adquiridos, objeto destas especificações, por todo o período do contrato.

9 DISPOSIÇÕES GERAIS

9.1 Os relatórios devem sempre ser apresentados em meio digital. Quando forem impressos por solicitação de ITAIPU deve ser utilizado o modo de impressão frente-verso.

10 MARCOS DE EVENTOS

10.1 Entrega de Certificação de profissionais: Em até 30 dias corridos a partir da Ordem de Início de Serviços, os documentos comprobatórios das certificações exigidas no subitem 7.1.

10.2 Entrega de Plano de Trabalho: Elaboração de um plano de trabalho e cronograma tentativo para as atividades a serem realizadas, em até 30 corridos dias após a OIS (Ordem de Início de Serviços).

10.3 Instalação e/ou atualização: Instalação e/ou atualização para última versão disponível

dos softwares detalhados no subitem 2.2, em até 45 dias corridos após a OIS.

11 CARACTERÍSTICAS GERAIS DO AMBIENTE TECNOLÓGICO

11.1 A CONTRATADA será considerada suficientemente conhecedora do ambiente tecnológico de ITAIPU, franqueando-se, desde já, quaisquer outras informações adicionais que a CONTRATADA julgar necessárias para consecução integral da sua solução. Não sendo, portanto, admitidas alegações em desconhecimento.

11.2 As versões dos softwares do ambiente tecnológico da ITAIPU poderão, a qualquer tempo, sofrer evolução de versão, de acordo com as necessidades da ITAIPU.

11.3 Principais ambientes operacionais:

11.3.1 Sistemas Operacionais:
a) AIX 5.3, AIX 7.2 e superiores;
b) Microsoft Windows 2003, 2008 e 2012 (Versões Server);
c) RedHat Enterprise Linux 6 e superiores;
d) Oracle Enterprise Linux e superiores.

11.3.2 Plataformas de Virtualização:
a) VMWare vSphere 6;
b) OracleVM 3.2 e superiores;
c) PowerVM e Particionamento Lógico (LPAR).

11.3.3 Banco de Dados:
a) Oracle;
b) SQL Server;
c) DB2;
d) MySQL Server;
e) PostgreSQL;
f) Adabas.

11.3.6 SAP ERP:
a) SAP ECC 6.0 Ehp7;
b) SAP Portal 7.4 R2;
c) SAP Netweaver 7.31 (BW);
d) SAP Solution Manager 7.2;
e) SAP Business Object 4.1.

11.3.7 Servidor de Aplicação:
a) Oracle WebLogic 10.3 JEE6;
b) IBM Websphere;
c) Red Hat JBoss.

11.3.8 Plataformas:
a) IBM Lotus Notes 9.0;
b) Natural/Adabas 6.1.1;
c) VetorH 6.2.31.47;
d) WebLogic 10.3 JEE6;
e) Outsystems 9 e superiores;
f) PHP 5.6.28;
g) Clarion 5.0 e 5.5;

h) Centura 4.1.0;
i) Tableau 10.4;
j) .NET;

11.3.9 Domínio:
a) Aproximadamente 4000 estações de trabalho Windows (7, 8, 8.1, 10);
b) Aproximadamente 180 servidores Windows;
c) Aproximadamente 650 servidores Linux;
d) Aproximadamente 100 servidores AIX, *BSD, entre outros;
e) Todos servidores Windows e *nix autenticam em um domínio.

11.3.4 Informações adicionais:
a) Diretório *OPENLDAP 2.4.39 e superiores*;
b) Samba 3.6.9 e 4.4.4 e superiores;
c) PAM: *Password Manager Pro*(PMP);
d) *Citrix*;
e) Servidores *WEB*: *Apache e IIS*;
f) Antivírus *Trend Micro*;
g) Firewalls Checkpoint 4800 com Algosec Firewall Analyzer;
h) Servidor de impressão *CUPS*;
i) Suíte de monitoramento e gestão de chamados IBM Tivoli;
j) Filtro de Conteúdo *BlueCoat*;
k) Todos os servidores inicializam via *SAN*;
l) Dois *Data Centers* distantes a aproximadamente 6 km, interligados por canais ópticos em FC e *Ethernet*.

11.4 Equipamentos INTEL e Estrutura de Armazenamento:

a) Quatro chassis HP c7000 com conexões FC SAN, e lâminas: HP Proliant BL620c G7 e HP Proliant BL480c G8;
b) Duas Unidades de Armazenamento EMC EMC VMAX 20K;
c) Duas unidades de equipamentos EMC VPLEX.