Brasília, 06 de dezembro de 2018.

**Ao**
**MINISTÉRIO DE MINAS E ENERGIA – MME**
**Coordenação-Geral de Tecnologia da Informação – CGTI**
**Brasília - DF**

**Ref.: Adesão a Ata de Registro de Preços N° 1/2017**
**Processo N° 00034.003796/2016-31**
**Pregão Eletrônico SRP N° 28/2017**

**Att.: Sr. Hiram Costa Botelho**
**Coordenação-Geral de Tecnologia da Informação**

Prezado Senhor,

Encaminhamos nossa Proposta Comercial para Adesão a Ata de Registro de Preços N° 1/2017, de Solução de Segurança composta por equipamentos de verificação e correlação de vulnerabilidades e de detecção e mitigação de ataques de negação de serviços distribuídos (DDoS), baseada em hardware e software, para proteção aos dispositivos e serviços de rede do Ministério de Minas e Energia, incluindo instalação, configuração e serviços de suporte técnico e manutenção por 36 (trinta seis) meses.

Agradecemos a oportunidade e colocamo-nos à disposição para esclarecimentos adicionais que se façam necessários.

Atenciosamente,

**Renan Pieratti**
**Diretor**
renan.pieratti@ttiinformatica.com

## 1. Detalhamento da Solução Ofertada

| ITEM | DESCRIÇÂO | QUANTIDADE |
|---|---|---|
| 1 | Solução contra ataques de DDoS do fabricante A10 Networks, marca A10 Networks, modelo Thunder 3030S-TPS, procedente dos EUA – Estados Unidos da América. | 01 |
| 2 | Serviços de Instalação, Customização e Transferência de Tecnologia | 01 |
| 3 | Suporte Técnico e Manutenção por 36 (trinta e seis) meses | 01 |

## 2. Descrição da solução de TI como um todo

Solução de Segurança composta por equipamentos de verificação e correlação de vulnerabilidades e de detecção e mitigação de ataques de negação de serviços distribuídos (DDoS), baseada em hardware e software, para proteção aos dispositivos e serviços de rede da Imprensa Nacional, incluindo instalação, configuração e serviços de suporte técnico e manutenção por 36 (trinta seis) meses, e serviços de Operação Assistida pelo período de 06 (seis) meses.

## 2.1 Requisitos da contratação

2.1. **Especificações técnicas** – Compreende a solução de segurança, os seguintes componentes e respectivas quantidades a serem adquiridas:

2.1.1. **Appliance, marca A10 Networks, modelo Thunder 3030S-TPS**

a) Composto de 01 (um) dispositivo de Hardware do tipo appliance e software licenciado, do mesmo fabricante, **A10 Networks** idêntico e com todas as funcionalidades;

b) Hardware dedicado tipo appliance com Sistema Operacional customizado para garantir segurança e melhor performance;

c) Gabinete para instalação em rack padrão 19 polegadas, possui altura de 1U (unidade de rack) por equipamento;

d) Será acompanhada de todos os cabos e suportes (gavetas e braços) necessários para a instalação do equipamento;

e) Fontes AC com voltagem de 110/220 e chaveamento automático;

f) O equipamento será fornecido com fonte de alimentação redundante e Hot-Swappable;

g) O equipamento será fornecido com ventilação (Fan) redundante e Hot-Swappable;

h) A solução oferecida possui 06 (seis) portas Ethernet 10/100/1000, específicas para as funções de mitigação contra ataques DDoS;

i) A solução oferecida possui 02 (duas) interfaces com velocidade 1Gbps do tipo SFP (Small Form Pluggable);

j) A solução oferecida possui 04 (quatro) interfaces com velocidade 10Gbps do tipo SFP (Small Form Pluggable);

k) A solução contempla 04 (quatro) Mini-GBICs com velocidade de 1Gbps do no padrão SFP para cobre ou fibra para serem instalados nos slots SFP do equipamento;

l) A solução contempla 08 (oito) Mini-GBICs com velocidade de 10Gbps no padrão fibra (SFP +) para serem instalados nos slots SFP do equipamento;

m) Suporta 10 (dez) Gbps de throughput de proteção contra ataques de DDoS;

n) Suporta proteção contra ataques de TCP SYN Flood com performance de 6 milhões de TCP SYNs por segundo;

o) Suporta 30 milhões de conexões (Camada 4 OSI) simultâneas transportadas pelo equipamento;

**p) Funcionalidades**

- Possui quantidade de memória e capacidade de processamento suficiente para atendimento de todas as funcionalidades e desempenho solicitados no Anexo I – Termo de Referência do Edital de Pregão Eletrônico SRP n° 28/2017. É extremamente desejável que ambos os processadores da solução – assim como as memórias RAM tenham características de maior robustez e confiabilidade – evitando-se soluções que usem processador e memórias RAM encontrados em equipamentos de uso comum (exemplo – Laptops e/ ou Desktops);
- A solução permite repositório redundante de versões de firmware – visando aumentar sua disponibilidade;
- Virá acompanhado de todas as licenças de software ou hardware necessárias para atendimento às funcionalidade exigidas no Anexo I do Edital;
- Todos os dados de performance são referente a versão de software mais recente;
- A solução oferecida possui 01 (uma) porta Ethernet 10/100/1000 Base T, especifica para a função de gerenciamento do equipamento. A tabela de roteamento desta interface é independente à de roteamento das interfaces de dados;
- A solução oferta 01 (uma) interface específica para acesso remoto – permitindo que seja possível ligar e desligar o equipamento de maneira remota – assim como ter acesso equivalente à porta Console sem a necessidade de equipamentos de terceiros;
- Permite a configuração da solução em alta disponibilidade (Cluster);
- Suporta solução de redundância de dispositivos em modo Ativo-Standby, de maneira que, em caso de falha de um dos equipamentos, novas conexões sejam remanejadas para o equipamento redundante;
- Está disponível na solução ofertada suporte a mecanismo para analisar quando da inicialização do mesmo se existem erros no hardware ou em qualquer módulo de software do sistema operacional. Em caso de confirmação de erro, a solução suporta registrar tal erro em Log e evitar finalizar o processo de inicialização;
- Agregação de portas baseado no protocolo LACP;

- A Solução de DDoS Mitigation suporta BFD (Bidirectional Forwarding Detection) de acordo com as RFCs 5880, 5881, 5882 e 5883 para rápida convergência de protocolos de roteamento dinâmico;
- Suporte na solução à IGMP versão 2;
- Suporta alteração do intervalo ou período global utilizado para detectar anomalias de tráfego;
- Transporta múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando tags de VLAN;
- Identifica de maneira dinâmica e estática a correspondência entre endereços MAC (Camada 2) e IP (Camada 3);
- Realiza roteamento estático, assim como roteamento dinâmico através de protocolo BGP;
- A plataforma suporta alterar o timeout de sessões sendo transportadas pelo mesmo;
- Permite redistribuição de rotas de forma dinâmica para rotas IPv4 e IPv6;
- O equipamento suporta aplicação de endereços IP de forma estática ou dinâmica (DHCP).
- O equipamento oferecido suporta endereços IPv4 e IPv6;
- A solução de DDos Mitigation suporta técnicas para minimizar Loops na rede. Tais técnicas poderão ser aplicadas de forma direta ou indireta na rede;
- Suporta mitigação de ataques que visam vulnerabilidades na Camada 2 OSI;
- Suporta mitigação de ataques que visam vulnerabilidades na Camada 3 OSI;
- Suporta mitigação de ataques que visam vulnerabilidades na Camada 4 OSI;
- Suporta mitigação de ataques que visam vulnerabilidades na Camada 7 OSI;
- A solução suporta bloqueio de tráfego com deformidades ou em desacordo com respectiva RFC – quando aplicável. Quando verificar a presença de tais anomalias, a solução bloqueará o transporte de tal tráfego anomalo e registrará tal bloqueio. A solução bloqueará as seguintes deformidades/ anomalias de tráfego na rede:
  - ✓ LAND Attack;
  - ✓ Empty Fragment;
  - ✓ Micro Fragment;
  - ✓ IPv4 Options;
  - ✓ Invalid IP Fragment;
  - ✓ Invalid IP Fragment Offset;
  - ✓ Invalid IP Header Length;
  - ✓ Invalid IP Flags;
  - ✓ Invalid IP TTL;
  - ✓ No IP Payload;
  - ✓ Oversized IP Payload;
  - ✓ Invalid IP Payload Length;
  - ✓ Invalid IP Checksum;
  - ✓ ICMP Ping of Death;
  - ✓ TCP Invalid Urgent Offset;
  - ✓ TCP Short Header;
  - ✓ TCP Invalid IP Length;
  - ✓ TCP Null Flags;
  - ✓ TCP Null Scan;
  - ✓ TCP SYN e FIN no mesmo pacote;
  - ✓ TCP XMAS Flags;

- ✓ TCP XMAS Scan;
- ✓ TCP SYN Fragment;
- ✓ z. TCP Fragmented Header;
- ✓ TCP Invalid Checksum;
- ✓ UDP Short Header;
- ✓ a1. UDP Invalid Length;
- ✓ b1. UDP Kerberos Frag;
- ✓ c1. UDP Port Loopback;
- ✓ d1. UDP Invalid Checksum;
- ✓ e1. Runt IP Header;
- ✓ f1. Runt TCP/UDP Header;
- ✓ g1. IP Tunnel Mismatch; e
- ✓ h1. TCP Option Error.

- A Solução permite a criação de listas negras (Black Lists) assim como listas brancas (White Lists) visando dinamizar a decisão de mitigação de tráfego potencialmente malicioso na rede – ou de respeitar determinada política de segurança. A solução permite a criação de tais listas de forma direta (configuradas no próprio equipamento) ou indireta (criadas externamente à solução e importadas para a plataforma de mitigação DDoS);
- A solução de DDoS Mitigation suporta a inclusão de tráfego em listas negras ou brancas de forma estática ou dinâmica. A inclusão de tráfego de forma dinâmica nas listas negras/ brancas realizarse-á – como consequência de autenticação de tráfego de rede pela plataforma de DDoS Mitigation, ou de limites previamente ultrapassados na plataforma;
- A Solução suporta a aplicação de regras de mitigação com base nos seguintes parâmetros:
  - ✓ Origem IP;
  - ✓ Destino IP; e
  - ✓ Combinação Origem + Destino IP;
- A solução suporta classificar tráfego com base em um IP de Origem de um Host ou de uma ou mais subredes de Origem – e tratar o conjunto de Hosts e /ou redes como um único objeto para proteção contra ataques de DDoS;
- A solução suporta classificar tráfego com base em um IP de Destino de um Host ou de uma ou mais subredes de Destino – e tratar o conjunto de Hosts e /ou redes como um único objeto para proteção contra ataques de DDoS;
- A solução suporta classificar tráfego com base na combinação de um IP de Origem + IP de Destino de um Host ou de uma ou mais subredes de Origem + Destino – e tratar o conjunto de Hosts e /ou redes como um único objeto para proteção contra ataques de DDoS;
- A solução suporta classificar tráfego baseado em tabela de Geolocalização de IPs de origem – permitindo à solução realizar proteção contra ataques de DDoS com base na localização geográfica do usuário. A solução permite a importação de tal tabela de Geolocalização. A solução suporta ainda a utilização de tabelas de Geolocalização de acordo com formatação IANA;
- A Solução permite a instalação na rede através das seguintes topologias:
  - ✓ Inline – seja em Camada 2 OSI ou Camada 3 OSI para tomada de decisões de mitigação. Caso aplicada desta forma, a solução de mitigação suporta de forma nativa ou externa bypass de tráfego de rede em caso de falha no mitigador;

  - ✓ Offline (out of band) – de forma que receba tráfego suspeito através de técnicas de redirecionamento de rede (exemplo – injeção de rotas BGP) e

tome ações de mitigação. Neste modelo de instalação, a plataforma de mitigação receberá o tráfego a ser inspecionado e devolverá o tráfego limpo à rede através de SNAT, GRE ou IpinIP; e
  - ✓ Tap – recebendo tráfego espelhado da rede com o intuito de monitorar/ detectar eventuais ataques sem bloquear tráfego diretamente;
- A solução de mitigação suporta a validação de integridade do tráfego através de processo de autenticação do mesmo. Caso o tráfego não passe nos testes de autenticação disponíveis na solução de mitigação de ataques DDoS, o mesmo será bloqueado, ou redirecionado na rede. A plataforma de mitigação de ataques DDoS suporta os seguintes testes de autenticação:
  - ✓ Autenticação de conexão TCP através de SYN Cookie;
  - ✓ Autenticação de conexão TCP através de retransmissão dentro de timeout pré-estabelecido;
  - ✓ Autenticação de conexão UDP através de retransmissão dentro de timeout pré-estabelecido;
  - ✓ Autenticação de consultas DNS através de retransmissão dentro de timeout pré-estabelecido;
  - ✓ Autenticação de consultas DNS através de uso forçado de DNS baseado em TCP. A solução de DDoS mitigation enviará respostas à consultas DNS baseadas em UDP com o bit TC (Truncated) forçando o usuário a reenviar a mesma consulta de DNS baseada em TCP; e
  - ✓ Autenticação de requisições HTTP através de cookie inserido pela plataforma de mitigação de DDoS. O cookie poderá estar inserido em uma resposta HTTP com código 302 (Redirect) ou em um Script Java;
- A plataforma de DDoS Mitigation oferece ferramentas para controle de ataques de flood na rede. As seguintes ferramentas serão suportadas pela plataforma:
  - ✓ Limitação de conexões (Camada 4 OSI) simultâneas em determinado intervalo ou período;
  - ✓ Limitação de novas conexões simultâneas (Camada 4 OSI) geradas em determinado intervalo ou período;
  - ✓ Limitação de quantidade de tráfego fragmentado (Camada 3 OSI) simultâneo gerado em determinado intervalo ou período;
  - ✓ Limitação de quantidade de pacotes (Camada 3 OSI) gerados em determinado intervalo ou período;
  - ✓ Limitação de quantidade de pacotes gerados em determinado intervalo ou período;
  - ✓ Limitação de novas requisições HTTP simultâneas (Camada 7 OSI) geradas em determinado intervalo ou período;
  - ✓ Limitação de novas consultas DNS simultâneas (Camada 7 OSI) geradas em determinado intervalo ou período;
  - ✓ Limitação de novos túneis SSL (Camada 4 OSI) gerados em determinado intervalo ou período; e
  - ✓ Limitação de renegociação de túneis SSL (Camada 4 OSI) gerados em determinado intervalo ou período.
- Para proteção do protocolo UDP, a plataforma de DDoS Mitigation suporta:
  - ✓ Filtro para estabelecer tamanho mínimo ou máximo de pacotes UDP permitido na rede;
  - ✓ Detecção de Spoofing UDP;
  - ✓ Proteção contra scanning de portas UDP; e
  - ✓ Proteção contra ataques de amplificação (reflection attack) tais como NTP Monlist Attack e DNS Amplification Attack.

- Para proteção do protocolo TCP, a plataforma de DDoS Mitigation suporta:
  - ✓ Limitação de quantidade de retransmissões SYN em determinado intervalo ou período;
  - ✓ Proteção contra ataques de tipo SYN Flood – através de ferramenta SYN Cookie;
  - ✓ Proteção contra scanning de portas TCP;
  - ✓ Limitação de quantidade de pacotes TCP com janela zero (Zero-Window TCP) em determinado intervalo ou período; e
  - ✓ Limitação de quantidade de pacotes fora de ordem em uma conexão TCP em determinado intervalo ou período.
- Para a proteção do protocolo DNS, a plataforma de DDoS Mitigation suporta:
  - ✓ Filtro para evitar que consultas do tipo "ANY" sejam transportadas pela rede;
  - ✓ Limitação de consultas DNS por domínio (FQDN) buscado;
  - ✓ Limitação de consultas DNS por tipo de registro buscado. São suportados limites por tipo A, AAAA, MX, NS, CNAME e SRV;
  - ✓ Filtro para bloquear consultas DNS anômalas (má formadas); e
  - ✓ Limitação de quantidade de respostas de tipo "NXDomain" enviadas.
- Para a proteção do protocolo HTTP, a plataforma de DDoS Mitigation suporta:
  - ✓ Proteção contra ataques de tipo SLOW READ e SLOW POST;
  - ✓ Proteção contra ataques de tipo Slowloris;
  - ✓ Limitação de requisições HTTP analisando a URI buscada. São suportados limites por URI que: Seja exatamente igual a uma string; Comece com uma string; Contenha uma string; e Termine com uma string;
  - ✓ Filtro para bloquear requisições HTTP anômalas (má formadas);
  - ✓ Filtro de requisições HTTP analisando o USER AGENT ou REFERER da requisição. Deverá ser suportado bloquear uma requisição HTTP por USER AGENT ou REFERER que: Seja exatamente igual a uma string; Comece com uma string; Contenha uma string; e Termine com uma string;
  - ✓ Selecionar qual a ação será executada pela plataforma de DDoS Mitigation. Entre as ações mínimas suportadas deverão estar DROP ou RESET;
- A solução de DDoS mitigation suporta mecanismo para proteção contra ataque POODLE em direção aos recursos protegidos detrás da plataforma;
- A plataforma suporta proteção de tráfego MPLS (Camada 2 OSI);
- A plataforma de DDoS mitigation suporta a utilização de expressões regulares (PCRE) para customizar o perfil de proteção para conexões TCP, UDP assim como para requisições HTTP;
- A plataforma permite criar exceções das regras de proteção de acordo com configuração específica de bypass de mitigação.

q) Gerenciamento – Os elementos da solução oferecem as seguintes funcionalidades de gerência:
- Acesso via SSH para acesso criptografado a console de gerência;
- Interface Gráfica via Web;
- Gerência via SNMP;
- Permite análise de dados assim como gestão da solução de mitigação através de API;
- Cliente DNS (resolver);
- Suporte à Netflow v9 e v10 (IPFIX);
- Suporte à SFLOW;

- Suporte a SNMP v1, v2c e v3;

- Os logs de sistema terão a opção de ser armazenados internamente ao sistema ou em servidor externo; e
- É capaz de exibir, permitir edição, upload e download de configuração em formato texto.

2.1.2. **Serviço de Instalação, Customização e Transferência de Tecnologia.**

a) Serão fornecidos serviços de instalação, configuração e customização para todo o ambiente proposto, após a transferência de tecnologia de toda a solução de segurança adquirida;

b) Serão fornecido serviço de transferência de tecnologia com carga horária de, 20 horas;

c) A transferência de tecnologia será de todos os componentes e funcionalidades da solução adquirida;

d) A transferência de tecnologia será realizada antes da instalação e implantação da solução de segurança;

e) A turma será de até 04 (quatro) pessoas;

## 3. PLANILHA DE COMPOSIÇÃO DE PREÇOS

| ITEM | DESCRIÇÃO | QTDE. | VALOR UNIT R$ | VALOR TOTAL R$ |
|---|---|---|---|---|
| 1 | Solução contra ataques de DDoS do fabricante A10 Networks, marca A10 Networks, modelo Thunder 3030S-TPS, procedente dos EUA. | 01 | 703.650,00 | 703.650,00 |
| 2 | Serviços de Instalação, Customização e Transferência de Tecnologia. | 01 | 11.990,00 | 11.990,00 |

| ITEM | DESCRIÇÃO | QTDE. | VALOR UNIT MENSAL R$ | VALOR MENSAL R$ | VALOR TOTAL R$ |
|---|---|---|---|---|---|
| 3 | Suporte Técnico e Manutenção 36 (trinta e seis) meses. | 01 | 2.775,00 | 2.775,00 | 99.900,00 |
| **VALOR TOTAL R$ 815.540,00 (oitocentos e quinze mil quinhentos e quarenta reais)** | | | | | |

Declaramos que no preço cotado estão inclusas todas as despesas que incidem direta e indiretamente sobre os serviços prestados, tais como impostos, taxas, tributos, insumos, mão-de-obra e outras.

# 4. CONDIÇÕES COMERCIAIS

## 4.1 Garantia

O prazo de Garantia dos Equipamentos cotados é de 36 (trinta e seis) meses na modalidade "On-Site", a partir da data de emissão do Termo de Recebimento Definitivo por parte do Ministério de Minas e Energia, e será prestada em Brasília – DF.

## 4.2 Suporte Técnico

A abertura dos chamados de atendimento a suporte técnico será efetuado pelo e-mail: atendimento@ttiinformatica.com, ou pelo Tel.: 61 30375885 e support@a10networks.com e 0800-0201547.

# 5. PRAZOS

## 5.1 Pagamento

O pagamento será efetuado a vista em até 10 (dez) dias após o faturamento.

## 5.2 Entrega

A entrega dos Produtos será em no máximo de 30 dias após a assinatura do Contrato e acordo com o subitem 2.4 do Anexo I do referido Edital.

## 5.3 Validade da Proposta

O prazo de validade desta proposta é de 30 (trinta) dias, corridos a contar da data de sua apresentação.

## 5.4 Dados da Empresa Proponente

**Razão Social:** TTI Informática Representação e Consultoria Ltda - ME.
**CNPJ/MF Nº** 08.437.917/0001-60
**Inscrição Estadual Nº** 07.484.050/001-02
**Endereço:** SHS Quadra 06, Conj. A, Bloco C, Salas 309 e 310 - Ed. Brasil 21
**CEP:** 70.316-109 – Asa Sul – Brasília/DF
**Telefone/Fax:** (61) 3037-5885 **Cel.** (61) 98424-7118
**e-mail:** **renan.pieratti@ttiinformatica.com**

## 5.5 Dados Bancários

**Dados Bancários**
**Banco:** ITAÚ
**Número:** 341
**Agência:** 5606
**Conta Corrente:** 11940-1
**Nome da Agência:** Brasília Asa Norte
**Endereço da Agência:** SEPN Quadra 504 Bloco C
**Cidade:** Brasília – DF

## 5.6 Responsável pela Assinatura do Contrato

**Responsável Legal da TTI INFORMÁTICA**
**RENAN PIERATTI**
**RG: 765.942 SSP/DF**
**CPF: 364.645.621-34**
**Endereço Residencial: SQNW 311 Bloco A Apt. 102 – Noroeste – Brasília – DF**
**Estado Civil: Divorciado**
**Profissão/Cargo: Administrador/ Diretor**

Atenciosamente,

**Renan Pieratti**
**Diretor**
**renan.pieratti@ttiinformatica.com**