Companhia de Entrepostos e Armazéns Gerais de São Paulo
Av. Dr. Gastão Vidigal, 1946
05316-900 - Vila Leopoldina - São Paulo - SP
Telefone: (11) 3643 3700
ceagesp@ceagesp.gov.br - www.ceagesp.gov.br

ESCLARECIMENTO-1

PROCESSO ADMINISTRATIVO **Nº 028/2019**

IDENTIFICAÇÃO DA LICITAÇÃO **DATA:**
Pregão Eletrônico nº 26/2019 30/08/2019

OBJETO:
Contratação de Serviços – Fornecimento de Link de Acesso Dedicado à Internet, conforme especificações constantes do ANEXO I – TERMO DE REFERÊNCIA.

Abaixo segue transcrito, o pedido de esclarecimento encaminhado via e-mail, por licitante interessado em participar no pregão eletrônico supra citado e a respectiva resposta fornecida pela área demandante da contratação.

Pergunta -1 : "5 Especificação dos Requisitos da Contratação

Item:
5.15. Quando solicitado pela CONTRATANTE, a CONTRATADA deverá disponibilizar serviço DNS Secundário (resolução direta e reversa), inclusive de maneira segura DNSSEC ("Domain Name System Security Extensions"), para os domínios já registrados no DNS primário da CONTRATANTE. O DNS Secundário deverá ser disponibilizado pela CONTRATADA no prazo máximo de 30 (trinta) dias após a solicitação da CONTRATANTE. Por ocasião da ativação, a CONTRATADA responsabilizar-se-á pela correta propagação dos endereços IP alocados a CONTRATANTE, englobando otimização de rotas e ajustes de sistemas DNS, inclusive quanto à resolução reversa.

Questionamento:

O item em questão solicita o serviço de DNSSec. Dentro deste item, fazemos as seguintes considerações referentes ao produto ofertado pela Telefonica Brasil: A solução que utilizamos é feita via parceiro e homologada dentro da Telefônica onde não existe custos de propagação, sendo fator único para o custeio e precificação a quantidade de ZONAS (pode se entender também domínios) a serem configurados no ambiente. Quanto aos demais fatores envolvidos são os benefícios da solução, estamos falando de proteções que vão além de simples solução DNS. Por exemplo entregamos sem custos adicionais a seguintes prevenções dentre outras:

• Autenticação de origem de dados DNS: garante que o destinatário dos dados possa verificar a origem.
• Negação autenticada da existência: isso diz ao resolvedor (responsável por traduzir o nome do domínio para um endereço IP) que um determinado nome de domínio não existe.
• Integridade de dados: isso garante ao destinatário de dados que os dados não foram alterados em trânsito.
• Ataques distribuídos de negação de serviço (DDoS): ataques DDoS de hoje estão se tornando mais sofisticados, atacando mais profundamente a camada de aplicativos, enquanto anteriormente eles afetavam apenas as camadas externas de rede e de transporte.
• Ataques de amplificação: ataque de amplificação é um tipo de ataque de reflexão*, que envolve inundar o DNS público com vários pacotes UDP (protocolo de datagrama do usuário), onde esses pacotes são inflados com o objetivo de travar servidores.

*O termo "reflexão" refere-se a quando os resolvedores de DNS obtêm uma resposta a um endereço IP falso, que é enviado como uma consulta DNS como parte do ataque.

Companhia de Entrepostos e Armazéns Gerais de São Paulo
Av. Dr. Gastão Vidigal, 1946
05316-900 - Vila Leopoldina - São Paulo - SP
Telefone: (11) 3643 3700
ceagesp@ceagesp.gov.br - www.ceagesp.gov.br

Com isso o licenciamento e custos estão baseado no número de zonas, e não no número de solicitações/requisições/propagações que possa ter no servidor ou banda de acesso.

Sendo assim questionamos: qual o quantitativo de zonas a serem divulgadas para que a composição da solução seja aderente ao que se pede? Podemos considerar 3 zonas para o atendimento do mesmo?"

Resposta-1: Informamos que pode ser considerado o limite de 3 zonas para atendimento do serviço DNSSec.

SP, 30/08/2019.

Maria Valdirene R.S. Carlos
Pregoeira