Manaus, 09 de setembro de 2024.

Ofício circular n° 52/2024 – COLIC/CIGÁS.

(Referente ao Edital Pregão Eletrônico n° 90030/2024 – COLIC/CIGÁS).

Senhores Licitantes,

Em resposta ao Pedido de Esclarecimento recebido por esta Companhia de Gás do Amazonas - CIGÁS, referente a **Pregão Eletrônico n° 90030/302024 – COLIC/CIGÁS - Contratação de empresa especializada na prestação de serviço de Centro de Operações de Segurança (SOC), conforme condições e especificações técnicas constantes neste Edital e seus Anexos**, informamos que:

Através do DESPACHO N. 117/2024 - GETIN/CIGÁS, segue a devida resposta.

Referente aos ITENS: 3.1. ESPECIFICACOES TECNICAS MINIMAS:

3.1.14. Para a análise de vulnerabilidades, executada durante a fase de descoberta, a CONTRATADA deve utilizar ferramenta que atenda, no mínimo, as seguintes características.

3.1.22. Realizar o gerenciamento de todo o ciclo de identificação e tratamento de vulnerabilidades, monitorando máquinas, redes, sistemas e aplicações em busca de pontos de fragilidade. Os itens abaixo deverão ser considerados pela solução de SIEM/SOC:

- 1 - COMPUTADORES - 200
- 2 - SERVIDORES FÍSICOS - 6
- 3 - SERVIDORES VIRTUAIS - 40
- 4 - SWITCHES -18
- 5 - FIREWALLS - 1
- 6 - ACCESS POINT – 7

Questionamento 01: Nosso entendimento é que, do ponto de vista de gestão de vulnerabilidades de equipamentos, a solução deverá ser dimensionada para a quantidade exata de 272 (duzentos e setenta e dois) ativos, conforme tabela descrita no item 3.1.22. Está correto o entendimento?

Resposta 1: Confirmamos que a solução de gestão de vulnerabilidades deverá ser dimensionada para a quantidade exata de 272 ativos, conforme descrita no item 3.1.22.

Referente aos itens: 3.1. ESPECIFICACOES TECNICAS MINIMAS:

3.1.14. Para a análise de vulnerabilidades, executada durante a fase de descoberta, a CONTRATADA deve utilizar ferramenta que atenda, no mínimo, as seguintes características:

Questionamento 02: Nosso entendimento é que, do ponto de vista de gestão de vulnerabilidades de aplicações WEB, a quantidade de aplicações web testadas deverá ser de até 5 (cinco) FQDNs ou URLs. Está correto o entendimento, caso não esteja correto, qual a quantidade de FQDNs ou URLs que deve ser considerada?

Resposta 2: O item se refere as atividades realizadas durante a aplicação do pentest e considera o escopo especificado no item 3.1.22

Referente aos itens: 3.1. ESPECIFICACOES TECNICAS MINIMAS:

3.1.8. Deve contemplar os serviços de Testes de Intrusão (Pentest) pelo menos duas vezes ao ano a fim de identificar e explorar vulnerabilidades, simulando ataques reais que serão realizados por profissionais identificados, certificados e capacitados, incluindo a elaboração e apresentação de relatórios detalhados contendo os métodos, técnicas e ferramentas utilizadas, bem como avaliação, diagnóstico e recomendações de correção das vulnerabilidades porventura encontradas. Os termos “Pentest”, "teste de penetração", "teste de intrusão" e "teste de invasão", são considerados sinônimos.

3.1.22. Realizar o gerenciamento de todo o ciclo de identificação e tratamento de vulnerabilidades, monitorando máquinas, redes, sistemas e aplicações em busca de pontos de fragilidade. Os itens abaixo deverão ser considerados pela solução de SIEM/SOC:

- 1 - COMPUTADORES - 200
- 2 - SERVIDORES FÍSICOS - 6
- 3 - SERVIDORES VIRTUAIS - 40
- 4 - SWITCHES -18
- 5 - FIREWALLS - 1
- 6 - ACCESS POINT – 7

Questionamento 03: Nosso entendimento é de que, no contexto dos testes de intrusão (Pentest), os ataques devem ser simulados com base nos grupos de equipamentos especificados na tabela do item 3.1.22, não envolvendo outro tipo de equipamento fora dos já listados na especificação técnica. Além disso, entendemos que somente 1 (um) SSID deve ser considerado para os testes de invasão de rede sem fio. Este entendimento está correto, caso nosso entendimento não esteja correto, quantos SSID devem ser considerados?

Resposta 3: Confirmamos que os testes de intrusão (Pentest) devem ser simulados com base nos grupos de equipamentos especificados na tabela do item 3.1.22, não envolvendo outros tipos de equipamentos. Em relação aos testes de invasão de rede sem fio, considerar os 2 SSIDs.

Referente ao item: 3.4.2.5. Resposta a incidentes de segurança, incluindo contenção, erradicação e recuperação de sistemas afetados;

Questionamento 04: Referente ao item supracitado, intendemos que as atividades descritas no item, deve ser executada pela equipe de segurança da CONTRATANTE, com o apoio e recomendações da equipe de segurança da CONTRATADA. Esta correto nosso entendimento?

Resposta 4: Seu entendimento está correto. As atividades de resposta a incidentes, incluindo contenção, erradicação e recuperação de sistemas afetados, serão executadas de maneira mútua e colaborativa, com o apoio e recomendações da equipe de segurança da CONTRATADA.

Referente ao Item: 3.3 THREAT HUNTING, onde cita:

Questionamento 05: Em relação ao item mencionado, considerando que o escopo dos serviços de Threat Hunting pode ser bastante amplo, gostaríamos de confirmar se as atividades dos profissionais designados para realizar os serviços propostos, com o suporte de ferramentas específicas, serão executadas de forma remota e durante o horário comercial. Está correto nosso entendimento?

Resposta 5: Confirmamos que as atividades de Threat Hunting, realizadas pelos profissionais designados e com o suporte de ferramentas específicas, poderão ser executadas de forma remota e durante o horário comercial, desde que isso não comprometa a efetividade e a qualidade dos serviços prestados e impactando o bom funcionando das atividades da Companhia conforme descrito no item 3.1.10

Questionamento 06: Entendemos a importância de tais certificações para garantir a segurança da informação e a confiabilidade dos serviços prestados. Entretanto, consideramos que uma empresa que esteja atualmente em processo de certificação na norma ISO 27001, com previsão de conclusão dentro dos próximos 12 meses, atende a essa necessidade. Sendo assim, acreditamos que a empresa vencedora deve garantir que todas as exigências da norma sejam cumpridas rigorosamente. Nesse sentido, ao apresentarmos declaração/documento oficial da empresa de consultoria que atesta o andamento do trabalho de implementação da ISO 27001 em nossa empresa, como forma de comprovar o andamento do processo de certificação, estaríamos atendendo ao especificado no item 6.1.1. do Termo de Referencia.

Adicionalmente, vale ressaltar que dentro do nosso quadro de profissionais, possuímos certificações de segurança relevantes, tais como, CISSP (Certified Information Systems Security Professional). Reiteramos nosso compromisso em obter a certificação ISO 27001 dentro do prazo mencionado e, desde já, colocamo-nos à disposição para quaisquer esclarecimentos adicionais.

Gostaríamos de salientar que a aceitação deste documento de consultoria como evidência temporária de cumprimento do requisito de certificação contribuirá para a manutenção da isonomia no processo licitatório. Isso porque possibilitará a participação de empresas que estão comprometidas com as melhores práticas de segurança da informação, mas que, por motivos de prazos de implementação, ainda não obtiveram a certificação final. Tal medida garantiria uma competição justa entre os participantes, sem comprometer a qualidade e a segurança exigidas no edital.

Está correto nosso entendimento?

Resposta 6: Entendemos o posicionamento em relação à certificação da família ISO 27000. No entanto, o Termo de Referência exige a apresentação de pelo menos uma das certificações listadas no item 6.1.1, no momento da licitação. A apresentação de um documento que comprove o andamento do processo de certificação não substitui a exigência da certificação.

Ressaltamos que a CIGÁS busca garantir a contratação de empresas com comprovada experiência e expertise em segurança da informação. A exigência de certificações específicas visa assegurar a qualidade e a confiabilidade dos serviços prestados.

Informamos que essas respostas estarão disponíveis no endereço eletrônico da CIGÁS e se tornarão parte integrante do Edital e seus anexos.

Por fim, como o presente expediente não acrescenta novas informações e exigências ao Edital e nem afeta a formulação da proposta de preços, a data designada para abertura do certame permanecerá inalterada.

Atenciosamente,

DANIEL SILVA DOS SANTOS
Pregoeiro da Comissão Permanente de Licitação – CPL/CIGÁS

Visto:

ODÍLIO MENDONÇA DA SILVA
Coordenador de Licitação – COLIC/CIGÁS