- Nº do processo: 4014.2025.DEMLPA.PE.0043.MPPE
- Nº do edital: 4014.2025.DEMLPA.PE.0043.MPPE
- Objeto: Ata de Registro de Preços para contratação de empresa para futura e eventual execução de SERVIÇOS DE SOLUÇÃO DE INFOVIA, com fornecimento e instalação de Links MPLS e operação de SDWAN (com BGP Self Healing) para conexão entre Recife e demais localidades, conforme Anexo I, Termo de Referência deste Edital.
- Início das propostas: 31/10/2025 08:00:00
- Termino das propostas: 18/12/2025 09:00:00

- Protocolo: 62DA9EE6-8006-4E2F-9F61-8196EFE96B87
- CNPJ / CPF: 05250796000154
- Tipo do Registro: Pedido de esclarecimento
- Razão social / Nome: NETWORK SECURE SEGURANCA DA INFORMACAO LTDA
- Data do registro: 15/12/2025 13:57:28
- Descrição: QUESTIONAMENTO 12:

  Itens 10.5.3.4.12.4.2 e 10.5.3.4.12.4.15

  Para atendimento do requisito de Penetration Test com publicação em site oficial e relatório público de testes independentes, o MPPE aceita: (a) publicação do sumário executivo do pentest do ambiente implantado no contrato (com relatório completo sob NDA), ou (b) exige especificamente pentest do produto/fabricante publicado no site do fabricante? O que o MPPE considera ‘site oficial’ (fabricante / contratada / órgão) e qual o nível mínimo de detalhe esperado no relatório público?

  QUESTIONAMENTO 13:

  Item 5.3 – 10.5.3.4.12.3 e subitens (fontes mínimas de coleta/integração)

  Para fins de dimensionamento e planejamento de implantação, solicita-se informar o quantitativo atual (aproximado) das soluções/fontes citadas no item 10.5.3.4.12.3 e subitens.

  QUESTIONAMENTO 14:

  Item 15.10.2.1.2.2.

  Considerando que o objeto envolve a operação de um SOC (Security Operations Center), entende-se que a certificação ISO/IEC 27001, quando utilizada como requisito, deve estar diretamente vinculada ao ambiente e aos processos do SOC (ex.: monitoramento, correlação e tratamento de eventos, gestão de incidentes, gestão de acessos privilegiados, registro e retenção de evidências, gestão de mudanças, continuidade e melhoria

contínua).
Isso porque uma ISO/IEC 27001 genérica (com escopo amplo e sem relação com a operação do SOC) pode não refletir a maturidade e o controle efetivo sobre as rotinas críticas do serviço contratado, enquanto uma certificação com escopo aderente ao SOC dá mais segurança à Administração quanto à existência de um SGSI aplicado exatamente onde o risco é maior: no processamento de logs, dados sensíveis e na tomada de decisão operacional durante incidentes.
Diante disso, solicitamos confirmar: a Administração exige que a ISO/IEC 27001 apresentada tenha escopo explicitamente aplicável ao SOC (ou às atividades essenciais do SOC), e que o certificado seja do ambiente/unidade responsável pela execução do serviço, e não apenas corporativo/genérico?