Pedido de Esclarecimento – PLAE 09/2025

Data: 12/06/2025

1. Sobre o Ambiente Técnico e Infraestrutura

1.1. Os endpoints e FQDNs informados (8.475 + 398) estão centralizados em uma rede única ou distribuídos entre filiais, redes OT, ambientes cloud e remotos?

Resposta: A rede é centralizada, mas está segmentada por meio de VLANs. No momento, não contamos com redes OTs.

1.2. A CODEMAR já utiliza alguma ferramenta de SIEM, EDR, firewall ou solução de Threat Intelligence com integração ativa? Se sim, quais?

Resposta: Atualmente, a CODEMAR e a Prefeitura não fazem uso de nenhuma ferramenta de SIEM ou EDR. A CODEMAR possui um Mikrotik operando como firewall, enquanto a Prefeitura iniciará a implantação do Firewall da Hillstone. Ambos os órgãos também não contam com soluções de Threat Intelligence.

1.3. Existe segmentação da rede entre ambientes de produção, administrativo e industrial? Há rede OT envolvida?

Resposta: Até o presente momento não dispomos de segmentação de redes de produção, administrativo e industrial. E não há rede OT envolvida.

2. Sobre Integração com o Ambiente Existente

2.1. A plataforma a ser contratada deverá substituir alguma solução atual, ou atuará como complemento/integrador de segurança?

Resposta: Não existe contrato atualmente. A solução a ser contratada atuará como complemento/integrador de segurança.

2.2. Há expectativa de integração com ferramentas/tecnologias existentes (ex: FortiGate, Trend Vision One, Microsoft Defender, Wazuh, etc.)? Se sim, poderiam informar as tecnologias atualmente existentes na pilha de segurança da informação?

Resposta: Estamos em fase final de contratação da empresa que fornecerá os serviços de internet que comtemplará o firewall da Hillstone.

3. Sobre Relatórios, Compliance e Governança
3.1. Quais frameworks ou modelos de conformidade a CODEMAR adota ou pretende seguir (ex: NIST, ISO 27001, LGPD, MITRE ATT&CK)?

Resposta: Atualmente, adotamos parcialmente a LGPD. A contratação pretendida tem como objetivo adequar a Administração à LGPD em sua totalidade, assim como aos frameworks e modelos de conformidade, como NIST e MITRE ATT&CK, com base em suas respectivas bases de conhecimento, conforme disposto no item 4.2.1.12.1 do Termo de Referência, além de atender às normas ISO 27.001 e ISO 27.002, conforme item 4.6.2.

3.2. Existem exigências específicas quanto ao formato e à periodicidade dos relatórios técnicos e executivos?

Resposta: De acordo com o previsto no Indicador TDM – Tempo de Disponibilidade Mensal, constante do item 6 do Termo de Referência, deverão ser entregues relatórios mensais para comprovar a execução dos serviços de forma consolidada. No entanto, uma das funcionalidades do sistema é a disponibilização integral dos relatórios na plataforma.

4. Sobre o Suporte Técnico e SLA
4.1. O suporte técnico especializado deverá ser prestado:

- (**X**) **Presencial eventual (O suporte deverá ser remoto e eventualmente Presencial)**
- ( ) 100% remoto
- ( ) Híbrido com escalas técnicas

4.2. Existe previsão de SLA para atendimento e resolução de incidentes (ex: crítico em 2h, médio em 6h)?

Resposta: Conforme previsto no item 4.4.6 do TR, Tempo para Resolução do Problema – TRP, dividido em três categorias de problemas, conforme o impacto:

- Alto: Solução em até 2 horas.
- Médio: Solução em até 6 horas.
- Baixo: Solução em até 24 horas.
- Meta por mês: ≥95%

4.3. A plataforma será operada por equipe interna da CODEMAR ou será necessário prover operação assistida por terceiros (SOC)?

Resposta: Ambos.

5. Sobre a Prestação dos Serviços Auxiliares

5.1. Haverá alocação mensal de horas técnicas para atividades como consultoria, investigação, resposta e análise? Qual a estimativa média mensal?

Resposta: Não haverá alocação mensal de horas técnicas para atividades como consultoria, investigação, resposta e análise.

5.2. Os serviços de pentest previstos deverão ser:

- ( ) Automatizados exclusivamente via plataforma
- (**X) Complementados com consultoria especializada e scripts personalizados**

5.3. O "planejamento e apoio à execução de testes de invasão" abrange redes externas (internet) e internas (LAN, DMZ)?

Resposta: Sim, toda a rede da organização.