Piracaia, 10 de junho de 2026

PARECER TÉCNICO – ANÁLISE PRELIMINAR DE INFRAESTRUTURA DE REDE E RECOMENDAÇÕES

Durante os atendimentos técnicos realizados na infraestrutura tecnológica do Instituto, foram identificadas recorrentes indisponibilidades de acesso a sistemas e portais governamentais em decorrência de bloqueios associados ao endereço IP público utilizado pela instituição.

Observou-se que a normalização do acesso ocorre após a substituição do endereço IP fornecido pela operadora de internet, indicando relação direta entre os bloqueios e a reputação do endereço IP em uso.

Como etapa inicial de diagnóstico, foram executados procedimentos de verificação e correção nos ativos da rede interna, incluindo atualizações de sistemas, verificações de segurança nos terminais de trabalho, análises de integridade dos equipamentos, validações de configuração e demais testes pertinentes à investigação do cenário apresentado.

Apesar das medidas adotadas, o comportamento relatado persistiu, não sendo possível identificar de forma conclusiva a origem dos eventos que ocasionam os bloqueios.

Adicionalmente, durante o processo de investigação foram recebidos registros de segurança indicando a identificação do endereço IP público institucional como origem de tentativas de autenticação classificadas como SSH Brute Force e FTP Brute Force contra hosts externos na internet.

Embora os registros disponíveis não permitam identificar com precisão qual ativo interno originou tais conexões, os eventos reforçam a necessidade de ampliação da capacidade de monitoramento, auditoria e rastreabilidade da infraestrutura atualmente em operação.

Atualmente, a rede possui serviços publicados externamente por meio de regras de NAT/Port Forward, incluindo o Portal da Transparência hospedado em ambiente local. Considerando as características do ambiente e os eventos reportados, não é possível, com os recursos atualmente disponíveis, determinar de forma precisa qual equipamento ou serviço está originando os comportamentos que vêm ocasionando a degradação da reputação do endereço IP institucional.

Diante deste cenário, recomenda-se a aquisição e implantação do equipamento MikroTik RouterBOARD RB4011iGS+5HacQ2HnD-IN, que passará a atuar como equipamento principal de borda da rede corporativa.

A implantação deste equipamento proporcionará:

- Monitoramento detalhado do tráfego de entrada e saída da rede;
- Registro e auditoria das conexões realizadas pelos ativos internos;

- Identificação de tráfego anômalo ou incompatível com a operação normal do ambiente;
- Controle centralizado das regras de NAT e publicação de serviços;
- Implementação de políticas avançadas de firewall;
- Geração de registros técnicos para análise de incidentes e rastreabilidade de eventos;
- Maior capacidade de identificação da origem dos eventos que possam impactar a reputação do endereço IP institucional.

Paralelamente à implantação do equipamento, serão realizadas ações de revisão e modernização da infraestrutura tecnológica atualmente em operação, com o objetivo de fortalecer os mecanismos de segurança, ampliar a capacidade de monitoramento e reduzir potenciais pontos de exposição.

Como medida complementar de diagnóstico, recomenda-se a suspensão temporária do acesso externo ao ambiente legado do Portal da Transparência por período determinado, mantendo-se monitoramento contínuo dos eventos de rede durante a execução do teste.

O objetivo desta ação é verificar eventual correlação entre a publicação do serviço e os bloqueios recorrentes observados, contribuindo para a identificação da causa raiz do problema.

As medidas propostas visam ampliar o nível de controle sobre a infraestrutura tecnológica, aprimorar a capacidade de auditoria dos eventos de rede e fornecer subsídios técnicos para a identificação definitiva da origem dos bloqueios atualmente enfrentados pela instituição.

Atenciosamente,

Guilherme Aparecido de Azevedo
Sócio
RG: 49.859.723-4/SSP/SP

Dyon Gonçalves
Sócio
RG: 46.789.032-8/SSP/SP