ASSEMBLEIA LEGISLATIVA
do Estado de São Paulo

PODER LEGISLATIVO

Requerimento de Informação n° 28/2026

Processo Número: **4373/2026** | Data do Protocolo: 24/02/2026 15:25:54

REQUERIMENTO DE INFORMAÇÃO

Nos termos do art. 20, XVI, da Constituição do Estado, combinado com o artigo 166 do Regimento Interno, requeiro que se oficie a Senhora Secretária de Meio Ambiente, Infraestrutura e Logística (SEMIL) do Estado de São Paulo, requisitando-lhe as informações a seguir:

1. **Medidas adotadas**

1.1. Quais providências imediatas foram tomadas pela Sabesp para conter o ataque e restabelecer os serviços?

1.2 Houve pagamento de resgate ou negociação com os criminosos?

1.3. Quais mecanismos de segurança digital foram implementados após o incidente para evitar novas ocorrências?

1. **Base de dados dos usuários**

2.1 Qual é o tamanho atual da base de dados de clientes da Sabesp (número de usuários cadastrados)?

2.2 Que tipo de informações pessoais e sensíveis estão armazenadas nessa base (ex.: CPF, endereço, histórico de consumo, dados bancários)?

1. **Risco de exposição de dados**

3.1. Existe confirmação de que os criminosos tiveram acesso às informações pessoais dos usuários?

3.2. Caso positivo, quais medidas estão sendo tomadas para proteger os clientes contra possíveis usos indevidos desses dados?

3.3 A Sabesp comunicou formalmente os clientes sobre o risco de exposição de suas informações?

4. **Transparência e acompanhamento**

4.1 Há relatórios técnicos ou auditorias independentes que comprovem a extensão do ataque e a eficácia das medidas adotadas?

4.2 A Sabesp pretende disponibilizar publicamente tais relatórios para garantir transparência à sociedade?

JUSTIFICATIVA

Apesar de o ataque cibernético contra a Sabesp ter ocorrido em outubro de 2024, torna imprescindível exigir informações detalhadas devido ao agravamento da situação global de cibersegurança. Empresas de infraestrutura crítica em diversos países têm sido alvo de ataques cada vez mais sofisticados, expondo dados sensíveis de milhões de cidadãos e colocando em risco serviços essenciais.

No entanto, o caso da Sabesp é ainda mais grave: trata-se de uma empresa privatizada que, ao priorizar resultados financeiros e dividendos, negligenciou investimentos robustos em proteção de dados e segurança digital. Essa postura fragilizou não apenas a companhia, mas também milhões de usuários que dependem de seus serviços.

O atraso em solicitar informações se justifica pela necessidade de avaliar, à luz do cenário internacional atual, se a Sabesp está realmente preparada para enfrentar novas ameaças digitais. A ausência de transparência e de investimentos adequados em segurança demonstra que os clientes podem estar vulneráveis, enquanto criminosos permanecem em poder de informações estratégicas.

Portanto, este requerimento não é apenas oportuno, mas urgente: exige da Sabesp explicações claras sobre como lidou com o ataque, qual a dimensão da base de dados exposta e quais medidas concretas foram tomadas para garantir que a negligência não se repita.

Emídio de Souza

PROTOCOLO DE ASSINATURA(S)

O documento acima foi assinado eletronicamente e pode ser acessado no endereço http://sempapel.al.sp.gov.br/autenticidade utilizando o identificador 320037003800380037003700 3A005000

Assinado eletronicamente por **Emídio de Souza** em **24/02/2026 15:14**
Checksum: **0465998464121382A85BD00BA3C5B4432C321BA2A075DFAC517E3ACFF70A394E**