

EMPRESA MUNICIPAL DE INFORMÁTICA S/A – IPLANRIO
EQUIPE DE PREGÃO
ESCLARECIMENTOS
PROCESSO IPL-PRO-2024/ 00034
CONSULTA PÚBLICA 001/ 2024

1 - No que diz respeito à exigência do subitem VIII - Exigências do serviço a ser contratado, está sendo requerido o cumprimento de SOC2 ou ISO 27001. Entendemos que a certificação ISO 27001 e a SOC2 são equivalentes e será aceita a comprovação de apenas uma delas. Nosso entendimento está correto?

R: Será exigida a apresentação de todas as certificações solicitadas em edital.

2 - Em relação à exigência do subitem VI - Resultados pretendidos: "Implementação de um processo estruturado de governança e gestão de riscos de segurança, com padrões e tecnologias adequadas para aumentar a proteção do ambiente", existe atualmente alguma documentação nesse sentido, ou será necessário que a CONTRATADAa elabore?

R: A contratada deverá elaborar o referido documento.

3 - Em relação à gestão de todas as soluções implantadas no ambiente da IPLANRIO, deve ficar claro o papel de cada CONTRATADA em caso de recuperação do ambiente em um possível ataque. Por exemplo, caso seja necessário tomar alguma ação envolvendo o BIG-IP, teremos acesso à solução ou apenas comunicaremos? Ressaltamos que, em caso de comunicação por meio da abertura de um chamado, o ambiente será impactado severamente.

R: As ações de resposta a incidentes serão construídas conjuntamente entre contratada e contratante, sendo algumas ações pré-aprovadas e realizadas pelo SOCe outras somente alertadas à contratante para tomada de decisão.

4 - Por favor, informe a quantidade de "take downs" por mês/ano e a quantidade de palavras-chave (termos) que devemos tratar em nossas ferramentas de inteligência contra ameaças.

R: Essas informações serão disponibilizadas em Estudo técnico preliminar e Termo de Referência no qual serão documentos disponibilizados em fase de cotação de preços.

5 - No item "VII:Exigências do serviço a ser contratado", solicita que a empresa comprove que possui processos implementados com base na norma ABNT NBR ISO/IEC 27001 e, também, apresente a certificação SOC2. Visto que o IPLAN tem a justa preocupação de que a empresa contratada possua processos implementados com base na norma ISO/IEC 27001, e que esta, devido a sua completude de escopo e pela adoção feita pela ABNT, direcionando a aplicabilidade ao mercado brasileiro, encontra uma adesão maior por parte das empresas nacionais e que, a certificação SOC2 solicitada neste item, possui escopo e abrangência similar a ISO/IEC 27001 (alguns artigos informam que as duas certificações compartilham entre elas mais de 95% dos mesmos controles de segurança) e, ainda, que um número expressivamente menor de empresas buscaram ser atestadas na SOC2 no Brasil, se compararmos com a quantidade de empresas que se adequaram e

possuem a certificação ISO/IEC 27001, recomendamos que a equipe do IPLAN-RJ avalie a alteração da certificação, exigida para este processo, de SOC2 para a ISO/IEC 27001.

R: Esta sugestão será avaliada, contudo, as certificações que serão exigidas para a qualificação técnica da licitante deverá ser exatamente a descritas e não similares ou semelhantes.