Contribuição e Manifestação da Funpresp-Exe acerca da Consulta Pública nº 2/2023

Nº	Instituição	Item	Contribuição	Área Responsável pela Manifestação	Resposta	Acatado		Alterações no	
						Sim	Não	Sim	Não
1	Be Safe Brasil	Item 2.1 - (Tabela: Grupo 1 - Item 3)	Com relação a consulta pública: https://www.funpresp.com.br/wpcontent/uploads/2023/11/Consulta-Publica-02.2023.pdf, referente ao item 3, o serviço a ser contratado trata-se de teste de invasão e não MONITORAMENTO DE ATAQUES CIBERNÉTICOS conforme consta no documento, essa nomenclatura dá a entender que é algum serviço relacionado a monitoramento como se fosse um SOC, e não a um serviço de ataque cibernético, a nomenclatura correta seria SERVIÇO DE TESTES DE INVASÃO (PENTEST). Se nos permitem gostaria de lhe fazer mais uma sugestão, no perfil dos profissionais exigidos para esse item. Para que tenham uma maior assertividade na contratação peçam certificações mais avançadas para esse serviço, por exemplo, colocaram no documento em questão o certificado de Linux, o que não garante que o profissional tenha conhecimento em ataques cibernéticos, este prova que sabe mexer em Linux, mas não garante que tenha competência para invadir um sistema. Os certificados CompTIA e Certified Ethical Hacker são equivalentes, dessa forma as exigências ficam limitadas, e de nível intermediário.	Gerência de Tecnologia e Informação	O serviço referente ao item 3 no grupo 1 consiste no MONITORAMENTO DE ATAQUES CIBERNÉTICOS. De acordo com o Item 9.10.1, é estipulado que os serviços gerenciados de segurança devem ser conduzidos por meio de um ambiente CSOC (Centro de Operações de Segurança Cibernética) próprio da CONTRATADA, contando com uma infraestrutura de datacenter própria ou terceirizada em provedores especializados. Por sua vez, o SERVIÇO DE TESTES DE INVASÃO é delineado no grupo 3, item 1. Os requisitos específicos para o perfil desse serviço estão detalhados no item 8.13.11 do Termo de Referência, no qual estão previstas as certificações Certified Expert Penetration Tester – CEPT ou GIAC, Certified Ethical Hacker – CEH, ou Certified Penetration Testing Professional – CPENT, entre outras.		**X**		**X**

			Sugerimos inserir no edital certificados de nível avançado como a CPENT- Certified Penetration Testing Professional, C|EH (Practical)- Certified Ethical Hacker (Practical) ou C|EH MASTER- Certified Ethical Hacker Master, dessa forma você terá uma garantia muito maior na qualidade da prestação desse serviço, pois são certificações de nível avançado.						

João Batista de Jesus Santana
Coordenador de Contratações e Aquisições