Nível de Classificação	Grupo de acesso
Público	**PRODAM**

PREGÃO ELETRÔNICO Nº 09/2024
(NÚMERO COMPRASNET 90009/2024)

PEDIDO DE ESCLARECIMENTO

Questionamento 12: Referente aos algoritmos de criptografia a serem utilizados na VPN, Diffie-Hellman Group 1, 2 e 5 são vulneráveis e a recomendação é substituir em implementações com IKEv2 por grupos superiores (14 em diante). Para IKEv1 ainda é possível utilizar o Group 5. Tendo os grupos 1 e 2 já não sendo suportados por diversos fabricantes nas versões mais recentes dos seus NGFW. Desta forma podemos desconsiderar os grupos 1 e 2?

Resposta 12: Agradecemos a sua observação pertinente sobre a vulnerabilidade dos grupos Diffie-Hellman 1, 2 e 5, e a recomendação de utilizar grupos superiores em implementações com IKEv2. Considerando que os grupos 1 e 2 já não são suportados por diversos fabricantes em suas versões mais recentes de NGFW, e tendo em vista a importância de garantir a segurança e a compatibilidade das soluções de VPN contratadas, concordamos em desconsiderar os grupos Diffie-Hellman 1 e 2 nas especificações técnicas do edital.

Manaus, 04 de setembro de 2024

HIAGO DIAS COSTA
Assinado de forma digital por HIAGO DIAS COSTA
Dados: 2024.09.04 09:16:55 -04'00'

Hiago Dias Costa
Comissão de Licitação