

Modulo TPM-SPI Asus



Modulo TPM-SPI Asus



Módulo TPM-SPI da Asus, essencial para segurança de dados e compatibilidade com sistemas operacionais modernos.

Classificação: Ainda não foi avaliado

Preço

Preço base com taxas 9,90 €

Preço de venda com desconto

Preço Venda 9,90 €

Desconto

[Ask a question about this product](#)

Descrição

O Módulo TPM-SPI da Asus é um componente crítico para aqueles que desejam aumentar a segurança de seus sistemas, especialmente em computadores que exigem um módulo Trusted Platform Module (TPM) para operações seguras, como criptografia de dados e autenticação. Este módulo é compatível com sistemas operacionais que necessitam de TPM para funções de segurança avançadas, como o Windows 11, que requer TPM 2.0 para instalação. O TPM-SPI da Asus fornece armazenamento seguro para chaves de criptografia, certificados digitais e senhas, além de ajudar na proteção contra ataques de malware e na verificação da integridade do sistema. A instalação é direta, conectando-se ao slot SPI TPM da placa-mãe Asus, e a ativação é feita através das configurações do BIOS/UEFI. Este módulo é ideal para atualizações de segurança em PCs mais antigos ou para garantir a compatibilidade com novos sistemas operacionais que priorizam a segurança.

Características Técnicas:

- Compatibilidade: Placas-mãe Asus com slot SPI TPM

- Tipo: TPM 2.0
- Interface: SPI
- Funções: Armazenamento seguro de chaves criptográficas, Certificação Digital, Proteção de dados
- Sistemas Operacionais: Windows 10/11, além de outros sistemas que suportem TPM
- Especificações:
 - Chip: Nuvoton NPCT750
 - Certificação Common Criteria EAL4+
 - Cumprimento FIPS 140-2
- Dimensões: 16 x 13 mm