



Criptografia por software

VS

Criptografia por hardware

HOSTING

Compartilha os recursos do computador para criptografar dados com outros programas no computador - apenas tão segura quanto seu computador.

Utiliza um **processador exclusivo** fisicamente localizado na unidade criptografada.

SENHA

Usa a **senha do usuário** como chave de criptografia para codificar dados.

O processador contém um **gerador de número randômico** para gerar uma chave de criptografia, chave essa que a senha do usuário deverá desbloquear.

Pode exigir atualizações de software.

ATUALIZAÇÕES

Melhor desempenho ao **retirar a criptografia** do sistema host.

DESCRIPTOGRAFIA

A criptografia por software é vulnerável a hackers devido a **fraca proteção contra ataques de força bruta** usando ferramentas on-line facilmente disponíveis.

Chaves de proteção e parâmetros de segurança crítica dentro do **hardware de criptografia**.

AUTENTICAÇÃO

A autenticação usa **recursos de sistema host**.

A autenticação ocorre no **drive criptografado por hardware**.

PROTEÇÃO

Vulnerável a ataques e é apenas tão seguro quanto o sistema host.

Proteção contra os ataques mais comuns, como ataques cold boot, códigos maliciosos e ataques por força bruta.

INSTALAÇÃO

A **compatibilidade** do Sistema Operacional pode variar.

Não exige nenhum tipo de instalação de software no PC host.

Pode ser implementada em **todos os tipos de mídia**.

FLEXIBILIDADE

A criptografia está **associada a um dispositivo específico**, assim a criptografia está sempre ativada.

CUSTO

Econômico para aplicações em ambientes **pequenos**.

Econômica para aplicações em ambientes **médios e grandes**, facilmente escalonável.

Pergunte a um Especialista

Planejar a solução certa de memória exige um conhecimento das metas de segurança do seu projeto. Deixe que os [especialistas da Kingston](#) te orientem sobre como melhor defender seus dados confidenciais.