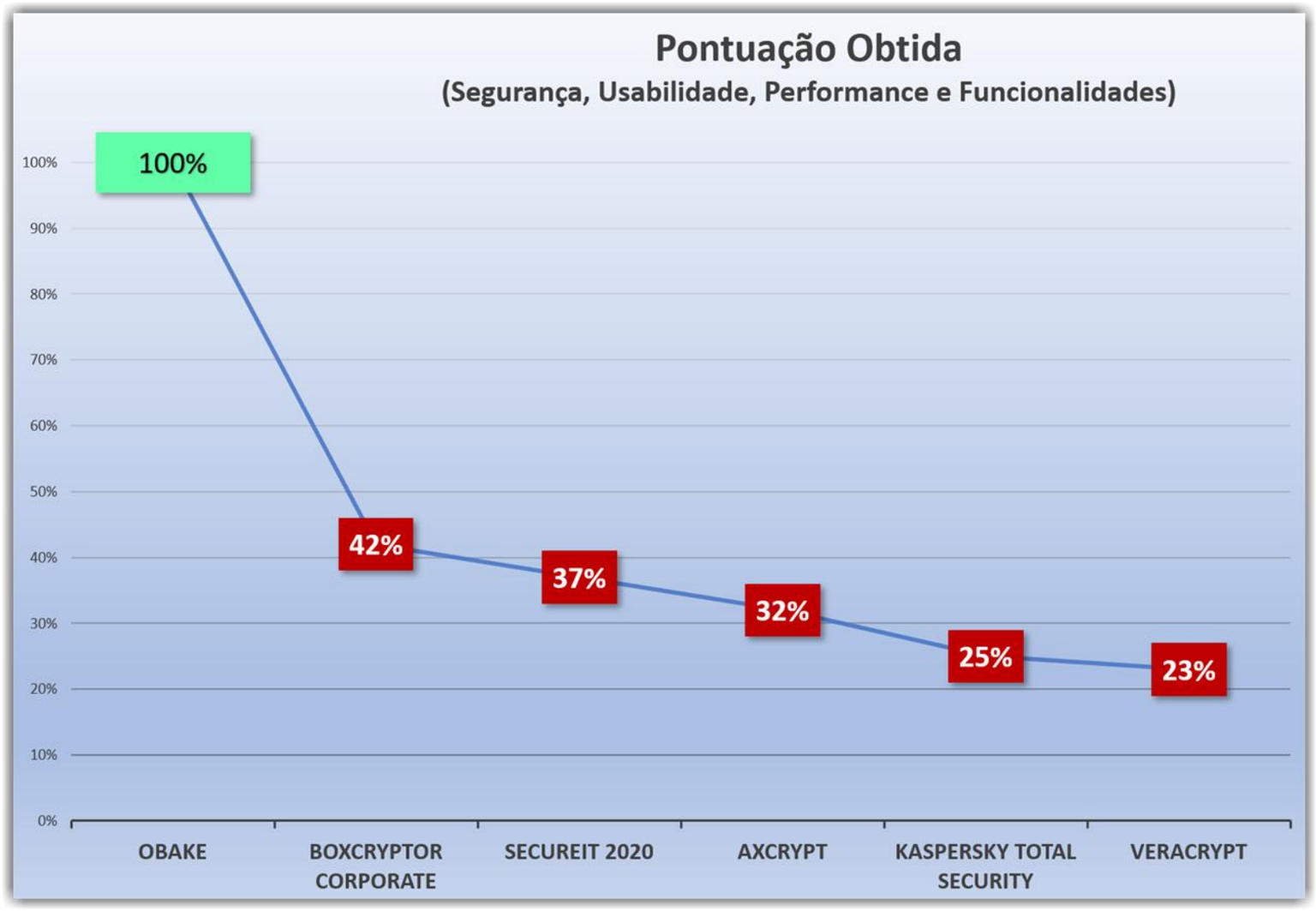
OBAKE

The Easiest and Powerful Encryption Suite for MS-Windows

TABELA COMPARATIVA 2025

Melhores Programas para Criptografia de Arquivos e Pastas



CARACTERÍSTICAS	OBAKE	Boxcryptor Corporate	SecureIT 2020	AxCrypt	Kaspersky Total Security	VeraCrypt
	100 %	42 %	37 %	32 %	25 %	23 %
Grande usabilidade e facilidade	✓	✓	✓	✓	✓	✓ [1]
Sem limites de arquivos	✓	✓	✓	✓	✓	✓
Manuseia arquivos maiores que 4Gb em sistemas de 32-bits	✓	✓	✓	✓	✓	✓
Trabalha com pastas e subpastas	✓	✓	✓		✓ [2]	
DIGITAL CERTIFICATES						
Criptografa usando Certificados Digitais	✓	✓				
Certificados: tamanho máximo da chave	8192 bits	4096 bits				
Tipo do Certificado	X509v3	RSA				
Aceita a cadeia ICP-Br	✓	✓				
Aceita certificados de Autoridades Públicas	✓	✓				
Aceita Certificados de Autoridades Privadas	✓	✓				
Imoprta e Exporta certificados facilmente	✓	✓		✓		
Certificados estocados com segurança na máquina usuária	✓	✓ [3]		✓ [3]		
Aceita certificado do usuário protegido por senha	✓	✓ [33]		8		
Aceita certificados estocados na Windows Store local	✓	28				
Aceita certificados “self-signed”	✓	✓				
Habilita carimbo-do-tempo com opção de servidores	✓					
Número ilimitado de destinatários	✓	✓		✓		
SECRET KEYWORDS						
Criptografa com chave-secreta	✓ [4]		✓	✓ [5]	✓	✓
Requer a chave-secreta a cada abertura de arquivo	✓		✓	6	✓ [7]	✓ [5]
Gera aleatórios diferentes para cada arquivo em operações de arquivos	✓		✓ [6]			
FUNCTIONALITY AND SECURITY						
Allows encrypted file sharing	✓	✓	✓	✓ [8]		✓ [9]
Permite compartilhamento sem links do fabricante	✓	28	✓	8	✓	
Permite compartilhamento por chaves-públicas.	✓	✓ [28]				
Dados de Autenticação embutidos nos arquivos [42]	✓	29				
Verifica arquivo criptografado após a finalização da criptografia	✓					
Permite checar o criador e pessoas autorizadas em arquivos	✓	✓ [28]				
Permite verificar Integridade, Autenticidade e Irretratabilidade	✓	✓ [28]				
Sanitiza arquivo de entrada automaticamente	✓		✓	✓		
Deleta arquivo de entrada automaticamente	✓	✓	✓	✓	✓	
Permite compressão inteligente com tamanho regulado pelo usuário	✓		✓			✓
Permite cancelar operações em curso	✓	✓	✓			
Permite rápida edição em arquivos criptografados [12]	✓	✓		✓	✓ [13]	✓ [13]
Recriptografia automática ao fechar arquivos	✓	✓		✓		
Permite manter a data/hora originais dos arquivos	✓	✓	✓	✓	✓	✓
Não exige a criação de pastas-seguras	✓		✓	✓		
Não exige Data-Vault (Cofres de Dados) [14]	✓		✓	✓		
Não exige serviços online nem Logins	✓	31	✓		✓	✓
Não permite acesso aos dados em smartphones	✓		✓		✓	
Permite senha de acesso às funções	✓	✓ [38]			✓	
Permite Autenticação de 2-Fatores para acesso às funções	✓	✓ [39]				
Conformidade com Zero-Knowledge	✓	✓ [32]	✓			✓
Permite restrições de acesso às configurações críticas [15]	✓	✓ [32]			✓	
Permite acesso seguro às configurações críticas [16]	✓	✓ [32]			✓ [17]	
Permite autorização compulsória por código [18]	✓					

OBAKE

The Easiest and Powerful Encryption Suite for MS-Windows

TABELA COMPARATIVA 2025

Melhores Programas para Criptografia de Arquivos e Pastas

Permite autorização compulsória com máximo de capilaridade [19]	✓	✓ [41]				
Permite envio de e-mail a cada mudança de configuração crítica [20]	✓	✓			✓	
Permite a criação de grupos de usuários para compartilhamento	✓	✓				
Permite a criação de grupos sem chaves-mestra [35]	✓					
Módulos de integração com Microsoft-365 [33]	✓					
Integração com Windows Explorer / Files Explorer	✓	✓		✓		✓
Permite sincronização com o One-Drive	✓	✓ [37]	✓	✓		
Permite sincronização com o Google-Drive	✓	✓ [37]	✓	✓		
Permite sincronização com o Dropbox	✓	✓ [37]	✓	✓		
Senhas de Acesso e Chaves são independentes	✓	[21]				
Sem acessos privilegiados (ADMIN)	✓	[32]	✓			✓
Permite troca ou eliminação de autorizações em arquivos	✓	✓		✓		
Protegido contra invasões do código	✓	✓ [40]	✓	?	✓	?
Protegido contra disassembly	✓	✓ [40]	✓	?	✓	?
Protegido contra desvios (code-hijack e code-hook)	✓	✓ [40]	✓	?	✓	?
ALGORITHMS						
Possui algoritmos para Conformidade ESG e Legal	✓	✓	✓	✓	✓	✓
Possui AES-NI para máxima performance e conformidade [43]	✓					
Possui AES-XTS para conformidade IEEE	✓					✓
Possui algoritmos modernos e seguros (XSalsa, ChaCha, Poly305, etc.) [44]	✓					
Possui algoritmo simétrico de nível militar (> 256 bits)	✓		✓ [22]			
Possui chaves “one-time” (não repetitivas)	✓ [24]	✓ [34]				
Tamanho das chaves do algoritmo simétrico	**32-65536 bits**	256 bits	448 bits	256 bits	56 bits	256 bits
Tamanha do HASH	**512 bits**	512 bits		256 bits		256 bits
Derivações seguras da chave informada [36]	5 [23]	2	1	1	1	1
PERFORMANCE						
Criptografia por OBAKE (2.39Gb) [25] [36]	**7,9 s**	22 s	154s	150 s	25 s	24 s
Decriptografia por OBAKE (2.39Gb) [36]	**7,7 s**	11,5 s	68s	55 s	9 s	21 s
Criptografia por AES-NI (2.39Gb) [25] [36]	**4,3 s**	22 s	154s	150 s	25 s	24 s
Descriptografia por AES-NI (2.39Gb) [36]	**4,8 s**	11,5 s	68s	55 s	9 s	21 s
Additional Features						
Conformidade com GDPR, LGPD, e outras leis e normas	✓	✓		✓	✓ [26]	✓
Conformidade com NIST-FIPS, ISO-IEC, RTF	✓	✓		✓	✓ [26]	✓
Resistente às leis de monitoração/inspeção de dados	✓			✓		✓
Permite auditoria no código-fonte	✓			✓		✓
Permite customizações nos algoritmos	✓					
	77	**32.5**	**28.5**	**24.5**	**19**	**18**

✓ = 1 ✓ = 0,5

1. O processo de configuração/instalação deve ser feito por equipe especializada e não é muito simples nem amigável. Definições iniciais podem causar perda de segurança e/ou performance, caso sejam feitas por leigos ou inexperientes em criptografia.
2. Ele copia pastas e subpastas para seu “cofre” – de fato não criptografa as pastas-e-subpastas originais, que deverão ser depois deletadas.
3. Os certificados do usuário/assinante estão estocados de forma insegura na máquina do usuário, criptografados com sua senha de acesso (c:\Users\<usuário>\AppData\Local\AxCrypt)
4. Essa funcionalidade deve estar liberada no ato do licenciamento. Empresas podem escolher quem terá (ou não) acesso à essa funcionalidade, com máxima capilaridade.
5. Ele não permite que o usuário defina uma “chave-secreta” por arquivo, mas trabalha com a senha de acesso utilizada para autorizar o aplicativo.
6. É pedida a senha da conta do usuário apenas na abertura do 1º arquivo – a partir daí, ela fica estocada em memória, dando condição a qualquer pessoa (ou programa) abrir arquivos protegidos sem exigência de autenticação.
7. Exige a chave de abertura “do cofre” apenas.
8. AxCrypt compartilha arquivos através de chaves públicas RSA-4096 bits estocadas automaticamente no seu servidor. Ele estoca as chaves-privadas para efeito de backup e sincronização entre dispositivos. Apesar da chave-privada estar criptografada com AxCrypt usando a senha definida pelo usuário, essa característica de usabilidade pode oferecer riscos: 1) o acesso ao produto é suficiente para abrir arquivos compartilhados (sem 2º ou 3º fatores de segurança); 2) como garantir que os certificados privados não são também estocados sem proteção?
9. Permite compartilhar arquivos-cofre mediante a informação da senha de acesso (o que enseja riscos). Não permite compartilhar partições criptografadas.
10. Permite compartilhar arquivos criptografados sem nenhuma interação com o fabricante ou terceiros – por exemplo, usando certificados-digitais dos destinatários e/ou chaves-secretas informadas previamente. No caso do BOXCRYPTOR, ele estoca todas as chaves utilizadas, tanto as simétricas (AES) quanto as assimétricas (certificados Público e Privado).
11. OBAKE não exige arquivos adicionais para compartilhamento. Todos os dados de cada usuário autorizado estão dentro do arquivo criptografado, sem risco nenhum de ataque e descriptografia sem o devido certificado privado do destinatário.
12. Permite abrir o arquivo criptografado no seu programa associado com apenas um clique/ENTER, recodificando-o automaticamente usando os mesmos parâmetros utilizados na criptografia do arquivo (chave ou certificado) e de forma transparente ao usuário.
13. O cofre deve estar aberto, expondo os outros arquivos contidos numa conexão de disco-virtual. Enquanto o cofre não for manualmente fechado, estará aberto para acessos via Explorer ou outros programas que usem as mesmas API’s.
14. Alguns programas exigem que seja criada uma pasta (ou um arquivo) que conterá todos os outros protegidos – por isso a denominação de “cofre” – obrigando o usuário a manter seus arquivos confinados nessa estrutura.
15. Funções críticas como compartilhamento compulsório, escolha de algoritmo, uso de chave-secreta, sanitização e outras podem estar restritas às modificações pelos usuários (BUSINESS).
16. O acesso às configurações críticas é feito por pessoal previamente autorizado e através de login e autenticação de 2-fatores. Essa autorização é dada por um programa à parte, protegido por senha e certificado exclusivo a cada empresa. Todas as operações performadas são informadas a quaisquer áreas ou pessoas previamente autorizadas, através de um LOG emitido por e-mail.

17. Apenas por senha de acesso que, se vazada, põe em risco os acessos ao ambiente.

18. As cópias podem ser “travadas dentro do código” para compartilhar qualquer dado criptografado entre pessoas ou áreas da empresa (exclusivamente), sem limite de quantidade. Tais compartilhamentos não podem ser deletados pelos times de TI (BUSINESS).

19. Cada área ou cópia pode, através de uma configuração restrita e segura, autorizar o compartilhamento da informação para pessoas ou áreas pré-determinadas, garantindo alta capilaridade nessa operação (CORPORATIVAS).

20. Configurações Restritas, acessadas apenas por pessoal autorizado (BUSINESS). Consulte também tópico 16.

21. Boxcryptor: todas as senhas, logins e demais autorizações são encadeamento de HASHes baseados na “password” informada pelo usuário, dando uma falsa sensação de segurança. O atacante não vai atacar os HASHes mas a senha criada pelo usuário (usualmente fraca).

22. Oferece o excelente Blowfish de 448 bits, apesar de não-conformidade com padrões estabelecidos.

23. OBAKE opera entre 5 e 11 diferentes chaves (depende do tamanho do dado): 1x 32 bits, 2x 65536 bits, 1x a 4x 512 bits, 1x a 4x 2048 bits.

24. Chaves criptográficas que independem da entrada do usuário, agregando componentes aleatórios e cálculos “on-way” para reforço de chaves inseguras.

25. Teste em 10 arquivos: 1 RAR de 2.3 Gb, 2 DOCX de 3.5 Mb cada, 1 XLSX de 10 Kb, 2 XLSX de 9 Kb cada, 1 PDF de 1.2 Mb, 1 PDF de 58 Kb, 1 TXT de 100 Mb, 1 TXT de 1 kb. OBAKE foi regulado para COMPRESSÃO OFF e VERIFICAÇÃO OFF para simular as mesmas operações que seus concorrentes. Algoritmos utilizados: OBAKE e AES-NI. Os tempos são meramente ilustrativos, podendo variar de acordo com o hardware utilizado e os programas em uso no momento do teste.

26. Em tese o programa usa e atende aos padrões citados, mas utilizando chaves de 56 bits apenas, põe em xeque a eficácia da proteção criptográfica proposta.

27. Não aceita o uso da Windows Store. A estocagem das chaves pode ser no servidor (criptografadas pelo HASH da senha) ou em modo local – nesse caso, o processo de compartilhamento é sacrificado.

28. Desde que compartilhando os arquivos-de-chaves (vide tópico 29) e usando o servidor Boxcryptor (vide tópico 27).

29. Todos os compartilhamentos são efetuados através de um “arquivo-de-chave” que embute a chave-simétrica AES utilizada no arquivo, criptografada com o certificado-digital público do usuário destinatário. Se o arquivo for compartilhado com 10 pessoas, haverá 10 arquivos adicionais independentes e relativos a cada pessoa. Todos os arquivos são criptografados por AES utilizando o HASH da senha-de-acesso do usuário. Um mesmo arquivo criptografado terá então “N” arquivos-de-chaves, em proporção direta com o número de usuários autorizados a visualizar o arquivo. Consulte também tópico 11.

30. Servidor exigido exclusivamente para: Compartilhamento de Arquivos e Pastas, Setup de um novo Dispositivo, Recuperação de Dados ou chaves, Criação/Edição/Deleção de Grupos, Sincronização. Descriptografia ou criptografia individual não requer servidor.

31. Pode-se configurar uma MASTER-KEY para os casos onde o(s) usuário(s) esquece(m) sua senha-de-acesso, da qual todos os HASHes e proteções derivam (vide tópico 28, 30). Sem essa MASTER-KEY a recuperação dos arquivos criptografados por esses usuários será impossível, caso não estejam compartilhados com outras pessoas e disponíveis no servidor Boxcryptor.

32. Caso a empresa tenha optado pelo ambiente servidor com MASTER-KEY (vide tópico 31), pode-se recuperar os certificados e dados criptografados através de um ataque de furto de credencial ou “insider enemy”.

33. Disponível na versão BUSINESS ou em módulo à parte (cópias PESSOAIS).

34. A proteção de acesso aos certificados, senhas e chaves segue padrão PBKDF2 com HMAC512 – um padrão seguro mas que, nesse caso, sempre será derivado da senha-de-acesso estabelecida pelo usuário.

35. Muitos programas utilizam uma “chave-comum” para criptografia de dados à grupos de usuários. OBAKE permite criar grupos onde cada indivíduo utilizará seu próprio certificado-digital, estando portanto cada componente do grupo sujeito a controles independentes atrelados a cada certificado (sigilo, disponibilidade e revogação do certificado). Além disso, traduz-se em melhor privacidade e maior economia (1 certificado pessoal vs vários certificados usados para cada grupo).

36. Não estamos considerando na pontuação a performance de disco nas operações de criptografia/descriptografia, nem o número de chaves utilizadas..

37. A integração é feita por triangulação com o serviço WHISPLY, que pode ser comandada pelo usuário ou através do aplicativo. Nesse caso, o usuário precisa informar os dados da conta (login/senha) para que o programa possa transmitir os arquivos. OBAKE (e outros) não exigem tais dados, funcionando “seamlessly” nas pastas que estejam compartilhadas/sincronizadas.

38. O programa exige o login/senha e possibilita o uso de um PIN de 4 caracteres/números. Nesse caso, além do PIN ser de tamanho insuficiente, não conta com autenticação de 2º fator.

39. Apenas nas cópias corporativas.

40. Bibliotecas adicionais não ofuscadas ou devidamente protegidas. Programa parcialmente protegido.

41. Apenas através de regras criadas no servidor Boxcryptor ou compartilhando regras do Active Directory.

42. A criptografia OBAKE com compartilhamento por certificados digitais embute todos os dados de autorização dentro dos arquivos criptografados. Isso se traduz em mais segurança e menor tamanho, além de ser muito menos burocratizada – não se exige que o usuário compartilhe endereços de e-mail ou arquivos-de-autorização para cada pessoa ou grupo autorizado. Além disso, preservamos uma característica que para nós é fundamental: nossa criptografia é realmente “end-to-end”; nada é transmitido ou enviado para nenhum servidor, garantindo absoluta privacidade ao usuário desde o momento da criação de um arquivo protegido.

43. AES-256-NI: algoritmo AES em total conformidade, estabelecido dentro de determinadas CPU’s a partir de 2010. A taxa de performance facilmente triplica em relação às melhores implementações em ASM/C++, por conta de não exigir BUS.

44. OBAKE oferece “ChaCha20-AEAD-Poly1305” (usado pelo Google em suas conexões seguras) e o “XSalsa-AEAD-Curve25519-Poly1305”, versão mais atualizada e forte do excelente algoritmo usado no TLS 1.3.