

Unidades cifradas por hardware Kingston IronKey - Soluciones de seguridad

Gestiona las amenazas y reduce los riesgos para datos móviles



Cuando los empleados utilizan sus propias unidades para almacenar datos corporativos o llevarse trabajo a casa, su organización se expone a grandes riesgos. Proteja los datos sensibles imponiendo el uso de unidades Flash USB cifradas por hardware o SSD externos Kingston® IronKey™. Por la posibilidad de elegir entre diferentes modelos y capacidades, estamos seguros de que encontrará la combinación ideal para las necesidades de su organización, tanto si lo que busca es la protección de los datos móviles como cumplir las directivas, leyes, estándares o normativas globales de datos en reposo o en tránsito, como el RGPD o la CCPA.

Todas las unidades IronKey cuentan con una garantía de cinco años (IronKey Vault Privacy 80 ES y la serie IronKey Keypad 200 cuentan con una garantía de tres años; IronKey D500SM cuenta con una garantía de dos años), soporte técnico gratuito y la legendaria fiabilidad de Kingston. Todas las unidades que se enumeran a continuación están totalmente cifradas por hardware, por lo cual son compatibles con las políticas de seguridad más estrictas. Para obtener más información, visite kingston.com/ironkey



Descripción de características	Serie IronKey Vault Privacy 50	IronKey Vault Privacy 80 ES	Serie IronKey Keypad 200	IronKey D300S	IronKey S1000
Número de referencia	IKVP50/xxGB USB-A IKVP50C/xxGB USB-C ¹	IKVP80ES/xxGB	IKKP200/xxGB	IKD500S/xxGB serializada IKD500SM/xxGB administrada	IKS1000B/xx GB Básico IKS1000E/xx GB Empresarial
Nivel de seguridad	Empresarial general	Empresarial general	Grado militar	Grado militar/Mejorado	Grado militar/Mejor de su categoría
Capacidades ²	8-512GB	480-7680 GB	8-256GB USB-A 8-512GB USB-C	8-512 GB	4-128GB
Modo de cifrado de hardware AES de 256 bits	XTS	XTS	XTS	XTS	Chip de cifrado integrado + XTS
Validación FIPS ³	FIPS 197	FIPS 197	FIPS 140-3 Nivel 3 (Pendiente)	FIPS 140-3 de nivel 3 (pendiente)	FIPS 140-2 Nivel 3
Contraseñas múltiples	Admin/Usuario/Recuperación de un solo uso	Admin/Usuario	Admin/Usuario	Administrador/usuario/recuperación de un solo uso	
Modo de frase de contraseña y longitud máxima	✓ Hasta 64	✓ Hasta 64	✓ Hasta 15	✓ Hasta 128	✓ Hasta 255
Símbolo de ojo para ver la contraseña introducida	✓	✓			
Firmware con firma digital	✓	✓	✓	✓	✓
Protección contra malware BadUSB	✓	✓	✓	✓	✓
Protección contra ataques de fuerza bruta a contraseña	✓	✓	✓	✓	✓
Compatible con la norma TAA	✓	✓		✓	✓
Preparado para el RGPD ⁹	✓	✓	✓	✓	✓
Acceso de solo lectura	✓	✓	✓	✓	✓
Protección contra manipulación		Microprocesador seguro con certificación CC EAL5+	✓ Epóxido	✓ Relleno de epóxido	✓ Relleno de epóxido
Doble partición oculta				✓	
Contraseña de criptoborrado	✓			✓	
Estanca al polvo/agua ⁴	IPx8		IP68	IP67, MIL-STD-810F	MIL-STD-810F
Opciones personalizables ⁵	✓		Programa de logotipo compartido	✓	
Teclado virtual	Windows® y macOS®	Pantalla táctil		Windows® y macOS®	Sólo Windows®
Opción administrada empresarial	Opción de administración local para pymes			✓ D500SM (SafeConsole)	✓ S1000E (SafeConsole)
PID personalizado - Compatible con extremo / DLP	✓			✓	
Material de la carcasa	Aluminio anodizado	Zinc y plástico	Aluminio anodizado	Zinc	Aluminio anodizado
Interfaz USB	USB 3.2 Gen 1	USB 3.2 Gen 1 External SSD	USB 3.2 Gen 1	USB 3.2 Gen 1	USB 3.1 Gen 1
Sistemas operativos compatibles					
Windows® 11, 10	✓	✓ Independiente del sistema operativo	✓ Independiente del sistema operativo	✓	✓
macOS® 11.x - 14.x	✓	✓ Independiente del sistema operativo	✓ Independiente del sistema operativo	✓	✓
Linux Kernel ⁶ v4.4+		✓ Independiente del sistema operativo	✓ Independiente del sistema operativo	✓ ⁷	✓ ⁸

1 USB tipo C® y USB-C® son marcas comerciales registradas de USB Implementers Forum.

2 Parte de la capacidad indicada de los dispositivos de almacenamiento Flash se emplea para formatear y para otras funciones, por lo tanto, no está disponible para el almacenamiento de datos. Consulte información más detallada en la Guía de memorias de kingston.com/flashguide.

3 Normas federales estadounidenses para el procesamiento de la información (FIPS, por sus siglas en inglés), publicación 140-2: "Security Requirements for Cryptographic Modules" (Requisitos de seguridad para módulos criptográficos). Consulte información más detallada en <http://csrc.nist.gov/publications/PubsFIPS.html>.

4 Certificación IEC 60529 para estanqueidad al agua con el tapón colocado. El producto debe estar limpio y seco

ESTE DOCUMENTO ESTÁ SUJETO A MODIFICACIÓN SIN PREVIO AVISO.

©2024 Kingston Technology Europe Co LLP y Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Reino Unido. Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469.

Reservados todos los derechos. Todos los nombres de empresas y marcas registradas son propiedad de sus respectivos dueños. MKF-501.19 ES

antes de su uso.

5 Para obtener más información, visite kingston.com/ironkey.

6 Compatible con comandos de Linux - Solamente procesadores basados en Intel i386/x86_64 y AMD - Funcionalidades limitadas.

7 IKD500S e IKD500SM: Compatible con sistema operativo Linux de 32 y 64 bits. Funcionalidades limitadas.

8 IKS1000B e IKS1000E: Compatible con sistema operativo Linux de 32 bits (y de 64 bits si se ha actualizado a la versión v6.x.x del software). Funcionalidades limitadas.

9 El cifrado puede formar parte del programa RGPD pero no garantiza el cumplimiento del RGPD.

