



Unidad Flash USB cifrada por hardware Kingston IronKey D500S

Certificado FIPS 140-3 de Nivel 3 (pendiente) con cifrado basado en hardware XTS-AES de 256 bits, resistente carcasa de zinc

La mejor unidad Flash USB Kingston IronKey™ D500S/SM incorpora la avanzada protección de grado militar que convierte a IronKey en la marca de máxima confianza para proteger información clasificada. Cuenta con la certificación FIPS 140-3 de Nivel 3 (pendiente), con nuevas mejoras del NIST que requieren actualizaciones seguras del microprocesador para reforzar la seguridad y las protecciones contra ataques para usos gubernamentales y militares. Los datos se cifran y se descifran dentro de la unidad D500S, sin dejar ninguna huella en el sistema anfitrión. Conjuntamente con el cifrado XTS-AES de 256 bits basado en hardware, se caracteriza por una sólida carcasa de zinc estanca al agua¹ y al polvo¹, resistente a las vibraciones y golpes según los estándares de grado militar², resistente al aplastamiento y rellena de epóxido para proteger a los componentes internos contra ataques de penetración.

IronKey D500S es un pilar esencial de las buenas prácticas de Protección contra pérdidas de datos (PPD/DLP), con la más estricta seguridad de grado militar, compatible con las leyes y reglamentos de cifrado de datos, como CMMC, SOC2, NIS2, FISMA, GDPR, PIPEDA, HIPAA, HITECH, GLBA, SOX, CCPA y TAA. D500S ofrece más funciones que cualquier otra unidad de su categoría, lo cual la convierte la solución de seguridad líder del sector para la protección de datos confidenciales de alto valor.

D500S realiza pruebas de autodiagnóstico al arranque y ante situaciones de recalentamiento o problemas de tensión, la unidad se apaga inmediatamente. Para mayor tranquilidad, D500S incorpora un firmware con firma digital, lo cual lo hace inmune al malware BadUSB. La protección contra ataques de fuerza bruta para adivinar contraseñas está siempre activada y, si se excede el número de intentos de empleo de contraseñas no válidas, la unidad se criptoborrará.

Además, ofrece una opción de contraseñas múltiples para acceder a los datos, que admite hasta tres contraseñas: Admin, Usuario y Recuperación de un solo uso. Con Admin se puede restablecer una contraseña de usuario y también especificar una

contraseña de recuperación de un solo uso si se olvida la contraseña de usuario.

D500S admite el modo tradicional de contraseña compleja o el modo de frase de contraseña³. Las frases de contraseña pueden tener entre 10 y 128 caracteres de longitud. El FBI recomienda frases de contraseña de varias palabras, de 15 o más caracteres, como método más resistente y más fácil de recordar que las contraseñas complejas.⁴

La unidad D500S incluye la opción Doble partición oculta, novedad en el sector, mediante la cual el administrador puede crear dos particiones seguras, de tamaño personalizado, para el administrador y el usuario. Esto posibilita un almacén oculto de archivos que puede emplearse para provisionar archivos a la partición del usuario según sea necesario. Cuando se utilizan sistemas que no sean de confianza o cuando se comparte la unidad, los Almacenes ocultos de archivos mantienen los datos protegidos e invisibles, salvo que se acceda a la misma de manera adecuada.

Con una secuencia especial de claves, el administrador puede introducir una contraseña de criptoborrado que criptoborrará la unidad destruyendo los datos para siempre y restableciéndola para impedir el acceso no autorizado en situaciones comprometidas.

Para ayudar a los usuarios con los problemas de teclado, todas las pantallas de introducción de contraseñas incluyen un símbolo de ojo, que mostrará la contraseña introducida para reducir los errores tipográficos. Se proporciona también un teclado virtual, disponible en inglés⁵, para ocultar la contraseña introducida de grabadores de pulsaciones de teclado y de pantalla.

Por otra parte, la unidad D500S también admite dos niveles de modos de Solo lectura (protección contra escritura). Tanto el administrador como el usuario pueden configurar el modo de Solo lectura en cada sesión para proteger a la unidad contra el malware de sistemas desconocidos. Además, el administrador puede establecer el modo de Solo lectura global, que configura la unidad en modo de Solo lectura hasta que es reconfigurada.

Además, se caracteriza por su rápido rendimiento de doble canal, aunque sin sacrificar la seguridad. La unidad incluye un número de serie exclusivo de 8 dígitos, que es el mismo que va electrónicamente grabado en la carcasa, con un código de barras escaneable, lo que facilita su implementación o para fines de auditoría.

La D500S ofrece numerosas opciones de personalización, es compatible con TAA/CMMC y se ensambla en EE.UU.

Modelo Managed (administrado)

Kingston IronKey D500SM (M = Administrado⁶) posibilita la administración centralizada del acceso y el uso de la unidad dentro de un conjunto de unidades en grandes empresas o administraciones públicas.

-
- Homologación FIPS 140-3 de Nivel 3 (pendiente), la más avanzada protección de grado militar
 - Opción de múltiples contraseñas con modos Compleja y Frase de contraseña
 - Opción Doble partición oculta, primicia en el sector
 - Contraseña de criptoborrado para situaciones comprometidas

- Sólida carcasa de zinc contra ataques de penetración, vibraciones y golpes según los estándares de grado militar, a prueba de polvo/agua IP67⁷
- Interfaz de uso sencillo
- Funciones completamente personalizables
- Disponible en modelo Administrado

Características Fundamentales

- USB cifrada por hardware de grado militar

Homologación FIPS 140-3 de Nivel 3 (pendiente) con cifrado XTS-AES de 256 bits y actualizaciones seguras de microprocesador para una mayor protección. Protecciones integradas contra ataques de BadUSB y de fuerza bruta Nueva función de autodiagnóstico de la unidad al arranque, protección térmica y de tensión que apaga automáticamente las unidades si alcanzan unos umbrales determinados.

- Opción de múltiples contraseñas para recuperación de datos

Permite habilitar las contraseñas de administración, de usuario y de recuperación de un solo uso. Con Admin se puede restablecer una contraseña de usuario y también especificar una contraseña de recuperación de un solo uso si se olvida la contraseña de usuario.

- Modo de contraseña compleja o de frase de contraseña

Se puede seleccionar entre los modos de Contraseña compleja o Frase de contraseña. Las frases de contraseña pueden ser oraciones complejas o conjuntos de palabras que solamente usted pueda recordar, de entre 10 y 128 caracteres de longitud. El símbolo de ojo para la introducción de contraseñas contribuye a reducir errores.

- Opción Doble partición oculta, primicia en el sector

El administrador puede crear dos Dobles particiones ocultas de tamaño personalizado para el administrador y para el usuario, para acceder a un Almacén oculto de archivos, lo cual permite mantener los datos protegidos e invisibles. Las dobles particiones ocultas aportan protección adicional en sistemas que no sean de confianza o cada vez que es necesario compartir la unidad.

- Contraseña de criptoborrado para situaciones comprometidas

La contraseña de criptoborrado borrará las claves de cifrado, eliminará todos los datos para siempre y restablecerá la unidad.

- Modos Sólo lectura global y Sesión (Prote. contra escritura)

Tanto el administrador como el usuario pueden configurar el modo de Sólo lectura en cada sesión para proteger a la unidad contra el malware de sistemas desconocidos. Además, el administrador puede establecer el modo de Sólo lectura global, que configura la unidad en modo de Sólo lectura hasta que es reconfigurada.

- Resistente carcasa según los estrictos estándares IronKey

Carcasa de zinc resistente al aplastamiento y rellena de epóxido para impedir las manipulaciones físicas. Certificación MIL-STD-810F para pruebas de caída, vibraciones y golpes. Certificación IP67 a prueba de agua¹ y polvo¹.

- N.º serie único de 8 dígitos y código de barras escaneable

Ahorro de tiempo tanto cuando la unidad está instalada como cuando se devuelve, así como durante las auditorías físicas.

- 100% personalizable

Activación, desactivación y modificación de las funciones y del perfil de la unidad. Logotipo compartido.

Especificaciones

Principales homologaciones	FIPS 140-3 de Nivel 3 (pendiente) MIL-STD-810F Compatible con TAA/CMMC, ensamblada en EE.UU.
Interfaz	USB 3.2 Gen 1
Capacidades*	8 GB, 16 GB, 32 GB, 64 GB, 128 GB, 256 GB, 512 GB
Conector	Tipo A
Velocidad ⁸	USB 3.2 Gen 1 8 GB – 128 GB: 260 MB/s en lectura, 190 MB/s en escritura 256 GB: 240 MB/s en lectura, 170 MB/s en escritura 512 GB: 310 MB/s en lectura, 250 MB/s en escritura USB 2.0 8 GB – 512 GB: 30 MB/s en lectura, 20 MB/s en escritura
Dimensiones	77,9 mm x 21,9 mm x 12,0 mm
A prueba de agua/polvo ⁹	Certificación IP67
Temperatura de servicio	0 °C a 50 °C
Temperatura de almacenamiento	-20 °C a 85 °C
Compatibilidad	USB 3.0/USB 3.1/USB 3.2 Gen 1
Opciones de personalización	D500S: Activación, desactivación y modificación de las funciones y del perfil de la unidad. Logotipo compartido. D500SM: Modificación del perfil de la unidad. Logotipo compartido.

Garantía/Asistencia	D500S: 5 años de garantía y asistencia técnica gratuita D500SM: 2 años de garantía y asistencia técnica gratuita
Compatible con	Windows® 11, 10, macOS® 11.x – 14.x, Linux ¹⁰ Kernel 4.4+

Números De Parte

Unidades serializadas

IKD500S/8GB
IKD500S/16GB
IKD500S/32GB
IKD500S/64GB
IKD500S/128GB
IKD500S/256GB
IKD500S/512GB

Unidades serializadas administradas

IKD500SM/8GB
IKD500SM/16GB

IKD500SM/32GB

IKD500SM/64GB

IKD500SM/128GB

IKD500SM/256GB

IKD500SM/512GB

Imagen Del Producto



* Parte de la capacidad indicada en un dispositivo de almacenamiento flash se emplea para formateo y otras funciones y, por tanto, no se encuentra disponible para el almacenamiento de datos. Por ese motivo, la capacidad de almacenamiento de datos real es inferior a la indicada en los productos. Para más información, consulte la [Guía de memoria Flash](#) de Kingston.

1. Consulte las especificaciones de la ficha técnica. El producto debe estar limpio y seco antes de su uso.
2. Certificación MIL-STD-810F para pruebas de caída, vibraciones y golpes.
3. El modo de frase de contraseña no es compatible con Linux.
4. De fbi.gov: [Oregon FBI Tech Tuesday: Building a Digital Defence with Passwords \(Martes tecnológico de FBI Oregón: Construir una defensa digital con contraseñas\)](#), 18 de febrero de 2020
5. Teclado virtual: solamente admite inglés (EE.UU.) en Microsoft Windows y macOS.
6. El servicio SafeConsole Management se contrata por separado.
7. El producto debe estar limpio y seco antes de su uso.
8. La velocidad puede variar en función del hardware, del software y del uso.
9. Homologación IEC 60529 IPX8, estanca con el capuchón puesto. El producto debe estar limpio y seco antes de su uso.
10. La compatibilidad con Linux es limitada. Consulte información detallada en el manual del usuario. Algunas distribuciones de Linux requieren privilegios de superusuario (raíz) para ejecutar correctamente los comandos de IronKey en la ventana de aplicaciones de terminal.

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. MKD-12192023

