



USB cifrada de Kingston / Ironkey Ventajas con respecto a BitLocker

BITLOCKER DE MICROSOFT 	USB CIFRADA DE KINGSTON / IRONKEY 
Característica	Ventaja de Kingston
<p>1. Compatibilidad limitada entre sistemas operativos:</p> <ul style="list-style-type: none"> - SOLAMENTE disponible en las ediciones Enterprise y Ultimate de Windows 7 Ediciones Pro y Enterprise de Windows 8.1 Windows 10. - Incompatible con Mac OS <p>2. Problemas con los parches/actualizaciones del sistema operativo</p> <ul style="list-style-type: none"> - Actualizaciones defectuosas; retrasos entre soluciones temporales <p>3. Vulnerable a "ROCA"</p> <ul style="list-style-type: none"> - Errores criptográficos en BitLocker - 'Peor que KRACK' - Google y Microsoft sacudidas por masivo defecto de cifrado de 5 años 	<p>1. Mejor compatibilidad entre sistemas operativos:</p> <ul style="list-style-type: none"> - Windows® 10 Windows 8.1 Windows 8 Windows 7 (SP1) Mac OS X v. 10.10.x - 10.13.x Linux Kernel v. 2.6. <p>2. Invulnerable ante los ataques de "ROCA"</p>
<p>1. Cifrado basado en el software</p> <ul style="list-style-type: none"> - Se ejecuta en el equipo host <p>2. Más vulnerable a los ataques</p> <ul style="list-style-type: none"> - Abierta a keylogging, sniffing, ataques hash y a la memoria 	<p>1. Cifrado basado en el hardware</p> <ul style="list-style-type: none"> - Protección totalmente integrada <p>2. No es vulnerable a ataques al software</p> <ul style="list-style-type: none"> - Elimina los intentos de rastreo y ataques hash y a la memoria <p>3. Firmware con firma digital</p> <ul style="list-style-type: none"> - No puede modificarse <p>4. Capa física de protección</p> <ul style="list-style-type: none"> - Las carcasas con envoltura/relleno epoxídico impiden el acceso a la memoria física
<p>1. Susceptible a los ataques de fuerza bruta</p>	<p>1. Protección contra 10 intentos de ataques de fuerza bruta</p> <ul style="list-style-type: none"> - Borra totalmente la unidad, o la desactiva <p>2. Impide que personas no autorizadas accedan a sus datos sensibles si la unidad USB se extravía o la roban</p>
<p>1. Requiere la intervención de los administradores de MIS/TI</p>	<p>1. Mínima intervención de MIS; fácil implementación</p>
<p>1. Utiliza normas tecnológicas obsoletas para las unidades USB</p> <ul style="list-style-type: none"> - AES de 256 bits, CBC (norma antigua) - Compatibilidad con FIPS (no homologada) <p>Nota: Las unidades cifradas con XTS-AES no serán accesibles en versiones de Windows más antiguas.</p> <p>Las unidades extraíbles seguirán utilizando los algoritmos de AES-CBC de 128 o de 256 bits.</p>	<p>1. Kingston utiliza las más recientes normas tecnológicas</p> <ul style="list-style-type: none"> - AES de 256 bits, XTS (norma más avanzada) - Con homologación FIPS 197 y FIPS 140-2 de Nivel 3 - Compatible con el RGPD de la UE - Cumple lo especificado por la norma 23 NYCRR 500 del NYDFS - Conforme a la normativa TAA

En síntesis: las unidades USB cifradas de Kingston / IronKey demuestran ser la solución óptima en materia de fiabilidad, compatibilidad y seguridad de soluciones de protección de datos móviles. Características: 100% compatibles con los reglamentos y normas más recientes | Funcionan con protección de terminales a efectos de DLP | No requieren software ni controladores | Diseñadas para una implementación rápida y eficiente.

