FIPS 140-2 y tecnología SED

Boletín de marketing

Preguntas más frecuentes

¿Qué es la norma FIPS 140-2?

FIPS (del inglés, *Federal Information Processing Standard*) 140-2 es una norma del gobierno estadounidense que describe los requisitos de cifrado y otros aspectos de seguridad relacionados que deben cumplir los productos informáticos para el uso de información confidencial, aunque no clasificada (SBU, del inglés *Sensitive But Unclassified*).

La validación FIPS 140-2 es un programa de certificación y pruebas que verifica que un producto cumple la norma FIPS 140-2. El National Institute of Standards and Technology (NIST) estableció el programa de validación de módulos criptográficos (CMVP, del inglés *Cryptographic Module Validation Program*) para validar productos conforme a estos requisitos.

¿Qué especifica la norma FIPS 140-2?

La norma garantiza el uso de prácticas de seguridad sólidas, como métodos y algoritmos de cifrado fuertes aprobados. También especifica cómo se debe autorizar el uso del producto a individuos y a otros procesos, y cómo los módulos o componentes deben estar diseñados para interactuar de forma segura con otros sistemas.

¿Por qué es necesario el cifrado?

Continuamente, las unidades de disco duro son sustituidas (por motivos de garantía, reparación y vencimiento del contrato de alquiler, con fines de ventas o porque las organizaciones desean destinarlas a otras tareas de almacenamiento), se pierden o son robadas. Cuando información no protegida escapa al control del usuario y se ve comprometida, las empresas deben hacer frente a pérdidas de ingresos, cuota de mercado y confianza de los clientes. Incluso pueden quedar expuestas a sanciones administrativas debido al incumplimiento de normas sobre la privacidad de datos. Esto puede ser catastrófico para una organización, especialmente si se trata de pequeñas y medianas empresas.

FIPS 140-2 y tecnología SED

Seagate calcula que, a diario, salen de los centros de datos alrededor de 50.000 unidades que almacenan terabytes de información. IBM calcula que el 90% de las unidades devueltas por motivos de garantía contiene datos legibles. Según expertos del sector, como el Ponemon Institute, el coste medio por filtración de datos aumenta a diario, con una media de 6,6 millones de dólares estadounidenses en 2008, o 202 dólares por cada registro filtrado.[1]

Ponemon Institute calcula además que el 81% de los ordenadores portátiles contiene datos confidenciales, y que el 10% de ellos se pierde o es robado a lo largo de su vida útil. Además, se calcula que cada semana se pierden o son robados 12.000 ordenadores portátiles sólo en aeropuertos de EE. UU. La desaparición de un equipo que almacena información confidencial no cifrada supone un coste medio para las empresas de casi 50.000 dólares estadounidenses. En casos extremos, los costes pueden ascender a cerca de 1 millón de dólares.[2]

¿Cuáles son los diferentes niveles asociados a la norma FIPS 140-2?

La norma FIPS 140-2 define cuatro niveles de seguridad. La validación FIPS 140-2 especifica el nivel de seguridad al que se ajusta el producto.

- El Nivel 1, que normalmente se utiliza en productos de cifrado de software exclusivamente, impone requisitos de seguridad muy limitados. Todos los componentes deben estar operativos y no deben existir fallos de seguridad flagrantes de diversos tipos.
- El Nivel 2 requiere autenticación basada en el cargo del usuario. (No se requiere la autenticación individual de los usuarios). También requiere la capacidad para detectar la intrusión física mediante sistemas de bloqueo físico o precintos de seguridad.
- El Nivel 3 añade resistencia a la intrusión física con fines de desmontaje o modificación, de manera que dificulta al máximo los ataques. Si se detecta la intrusión, el dispositivo debe ser capaz de borrar los parámetros de seguridad críticos.

  El Nivel 3 también incluye protección criptográfica eficaz y administración de claves, autenticación basada en la identidad y separación física o lógica entre las interfaces a través de las que se accede a los parámetros de seguridad crítica y se sale de ellos.
- El Nivel 4 incluye protección avanzada contra intrusiones y está diseñado para productos que operan en entornos desprotegidos físicamente.

¿Qué nivel de FIPS 140-2 ha obtenido Seagate?

Las unidades de almacenamiento con autocifrado (SED) de Seagate® han recibido la validación como unidades conformes con el Nivel 2 de la norma FIPS 140-2.

¿Por qué ha obtenido Seagate la validación de Nivel 2 de la norma FIPS 140-2?

Cada vez son más las organizaciones de todo tipo que requieren el cifrado de los datos almacenados para protegerlos de pérdidas o robos. La validación FIPS 140-2 de Nivel 2 se considera una marca de seguridad y calidad, y certifica a todos los compradores que las unidades SED FIPS de Seagate cumplen los requisitos del gobierno federal de los EE. UU. en relación con los productos de seguridad.

¿Cómo puedo saber si mi dispositivo de almacenamiento de Seagate cumple la norma FIPS-2?

Todos los dispositivos que cumplen la norma FIPS 140-2 utilizan mecanismos físicos de seguridad para detectar la intrusión física. Para averiguar si su dispositivo de almacenamiento cumple la norma FIPS-2 busque los precintos de seguridad ubicados en la parte externa.

¿Cómo configuro mi unidad SED FIPS de Seagate para garantizar el cumplimiento de FIPS-2?

Para configurar un dispositivo que cumpla con FIPS 140-2, consulte la política de seguridad del dispositivo entrando en el sitio web de validación de módulos NIST Module Validation List en http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm. Encontrará un procedimiento detallado para inicializar su dispositivo en la sección Secure Initialization (inicialización segura) del documento Security Policy (política de seguridad).

¿Para qué tipo de productos es aplicable la norma FIPS 140-2?

La norma FIPS 140-2 se aplica a cualquier producto capaz de almacenar o transmitir información confidencial. Esto incluye productos de hardware, como cifradores de vínculos, discos duros, memorias flash y otros soportes de almacenamiento extraíbles. También incluye productos de software que cifran datos durante su transporte o mientras están almacenados.

[1] Ponemon Institute, 2008 Annual Study: U.S. Cost of a Data Breach, febrero de 2009, www.ponemon.org, publicado en Data-breach costs rising, study finds, por Ellen Messmer, Network World, 02/02/09.
[2] Estudio de Intel: Stolen Laptops Cost to Business; eWeek, 23 de abril de 2009; Ponemon Institute Study, abril de 2009.

FIPS 140-2 y tecnología SED

¿Realmente necesito tanta seguridad? ¿No es suficiente con el sistema operativo?

La seguridad del sistema operativo, como las contraseñas, se puede burlar fácilmente extrayendo el disco duro e instalándolo en otro ordenador. Incluso las contraseñas del BIOS de las unidades de disco duro ATA son vulnerables si no se utilizan en combinación con dispositivos como la unidad SED de Seagate. Cifrar los datos del disco duro o el soporte de almacenamiento es un método de protección demostrado.

¿Qué organizaciones o empresas deben cumplir con la norma FIPS 140-2?

En EE. UU., el NIST exige a todas las agencias federales el uso de productos con certificación FIPS 140-2 Level 2 Validated para proteger los datos denominados *confidenciales pero no clasificados (SBU)* en sistemas informáticos y de telecomunicaciones (incluidos los sistemas de voz).[3] En Canadá, el Communications Security Establishment (CSE) exige a las agencias federales el uso de módulos con cifrado y certificación FIPS 140-2 Level 2 Validated para proteger los datos denominados *información protegida* (A o B) en sistemas informáticos y de telecomunicaciones (incluidos los sistemas de voz). La validación FIPS 140 también es un precursor necesario para que un producto criptográfico aparezca en la lista de productos precalificados como ITS del gobierno canadiense.[3] En Reino Unido, el Communications-Electronics Security Group recomienda el uso de módulos criptográficos con validación FIPS 140 Validated.[4]

También deben cumplir con la norma todas las empresas a nivel mundial relacionadas contractualmente con organizaciones de los gobiernos federales de EE. UU., Canadá o Reino Unido que deben cumplir el cifrado FIPS 140-2. Adicionalmente, a las empresas comerciales de todo el mundo, especialmente en los sectores financiero, sanitario, educativo y de infraestructuras (seguridad nacional), se les exige, cada vez con mayor frecuencia, el cumplimiento de la norma FIPS 140-2. Su intención es seguir el estándar más elevado en protección de datos. Reconocen el rigor que implica una certificación FIPS-140, considerada la mejor elección en materia de seguridad, y optan por cumplir esta norma para sus propias necesidades de cifrado.

www.seagate.com

¿Qué se necesita para obtener una certificación FIPS 140-2?

Para que un producto obtenga FIPS 140-2 Validated, debe adherirse a los requisitos de diseño e implementación establecidos y ser probado y aprobado en uno de los 13 laboratorios independientes acreditados por el NIST.

¿Cuál es la norma FIPS 140 vigente?

Las publicaciones FIPS con numeración 140 son un conjunto de normas de seguridad que especifican los requerimientos para los módulos de criptografía. La norma FIPS 140-1 se publicó en 1994, pero fue reemplazada por la norma FIPS 140-2, que es la norma actual, publicada en 2001. La norma FIPS 140-3 es una nueva versión en fase de desarrollo desde 2005. Se publicó un borrador en diciembre de 2009, pero aún no se ha lanzado para la validación de productos.

¿Existe una lista de productos con certificación FIPS 140-2 Validated?

El NIST conserva una lista de todos los productos disponibles comercialmente que cuentan con certificación FIPS 140-2 Validated.

Visite: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm

[3] http://csrc.nist.gov/groups/STM/cmvp/index.html
[4] www.cesg.gov.uk/

Incluye FIPS 140-2

AMÉRICA Seagate Technology LLC 10200 South De Anza Boulevard, Cupertino, California 95014, United States, +1 408 658 10 00
ASIA/PACÍFICO Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, +65 6485 3888
EUROPA, ORIENTE MEDIO Y ÁFRICA Seagate Technology SAS 16–18, rue du Dôme, 92100 Boulogne-Billancourt, Francia, +33 1 41 86 10 00

© 2013 Seagate Technology LLC. Todos los derechos reservados. Impreso en EE. UU. Seagate, Seagate Technology y el logotipo Wave son marcas comerciales registradas de Seagate Technology LLC en Estados Unidos y/o en otros países. El logotipo FIPS es una marca de certificación del NIST, lo que no implica la recomendación del producto por parte de NIST o los gobiernos de EE. UU. o Canadá. Todas las demás marcas comerciales o marcas comerciales registradas pertenecen a sus respectivos propietarios. La exportación o reexportación de hardware o software que contenga cifrado deberá cumplir la normativa del Department of Commerce, Bureau of Industry and Security de EE. UU. (para obtener más información, visite www.bis.doc.gov) y la importación y el uso fuera de EE. UU. deberán estar controlados. Seagate se reserva el derecho a modificar las ofertas o especificaciones de los productos sin previo aviso. MB605.2-1302ES, febrero de 2013