

A decorative graphic on the left side of the page features a large green circle partially overlapping a dashed black circle. Below these, there are several thin, concentric white circles that fade out towards the bottom. A small solid green circle is positioned above the dashed circle.

Boletín de marketing

Tecnología de la unidad FIPS 140-2 estándar y con autocifrado

Preguntas más frecuentes

¿Qué es la norma FIPS 140-2?

FIPS (del inglés, *Federal Information Processing Standard*) 140-2 es una norma gubernamental 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.

¿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 se pierden o son sustraídas o 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). 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.

- 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 por ciento de las unidades devueltas por motivos de garantía contienen 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

El Ponemon Institute calcula además que el 81% de los ordenadores portátiles contienen datos confidenciales, y que el 10% de ellos se pierde o sustrae. Adicionalmente, se calcula que cada semana se pierden o sustraen 12.000 ordenadores portátiles sólo en

¹ Ponemon Institute, *Estudio anual de 2008: Coste de la filtración de datos en EE.UU.*, febrero de 2009, www.ponemon.org, publicado en *Data-breach costs rising, study finds*, por Ellen Messmer, Network World, 02/02/09.

Tecnología de la unidad FIPS 140-2 estándar y con autocifrado



Preguntas más frecuentes

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 brechas 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.

¿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.

¿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 de unidades de disco duro BIOS 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 los EE. UU., el National Institute of Standards and Technology exige a todas las agencias federales el uso de productos con validación FIPS 140-2 de Nivel 2 para proteger los datos denominados *confidenciales pero no clasificados* en sistemas informáticos y de telecomunicaciones (incluidos los sistemas de voz).³ En Canadá, la Communications Security Establishment (CSE) exige a las agencias federales el uso de módulos criptográficos con validación FIPS 140-2 de Nivel 2 para proteger los datos denominados *información protegida* (A o B) en

² Estudio de Intel: Coste del robo de portátiles para las empresas; eWeek, 23 de abril de 2009; Estudio de Ponemon Institute, abril de 2009.

³ <http://csrc.nist.gov/groups/STM/cmvp/index.html>

Tecnología de la unidad FIPS 140-2 estándar y con autocifrado



Preguntas más frecuentes

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 140.⁴

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.



Incluye FIPS 140-2

¿Qué es la validación FIPS 140-2?

La validación FIPS 140-2 es un programa de certificación y pruebas que verifica que un producto cumple la norma FIPS 140-2. El NIST estableció el Programa de Validación de Módulos Criptográficos (CMVP, por sus siglas en inglés) para validar los productos en base a estos requisitos.

¿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 es probable que falte todavía un año para que sustituya a la norma FIPS 140-2.

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

El NIST conserva una lista de todos los productos disponibles comercialmente que cuentan con FIPS 140-2 Validated. Visite: <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm>

¿Por qué la certificación FIPS 140-2 es tan importante para los distribuidores de Seagate?

Los distribuidores de Seagate pueden utilizar FIPS 140-2 Validated como una herramienta eficaz para demostrar la calidad y las funciones de seguridad crítica que otros productos no tienen. Es una forma importante de marcar la diferencia de cara a los compradores de hoy en día preocupados por la seguridad.

³ <http://csrc.nist.gov/groups/STM/cmvp/index.html>

⁴ www.cesg.gov.uk/

www.seagate.com

Llamada gratuita: 00 8004 SEAGATE (732 4283)

(llamada no gratuita: 001 405 324 4714)

AMÉRICA
ASIA/PACÍFICO
EUROPA, ORIENTE MEDIO Y ÁFRICA

Seagate Technology LLC 920 Disc Drive, Scotts Valley, California 95066, EE. UU., +1 831 438 6550
Seagate Singapore International Headquarters Pte. Ltd. 7000 Ang Mo Kio Avenue 5, Singapur 569877, +65 6485 3888
Seagate Technology SAS 16-18 rue de Dôme, 92100 Boulogne-Billancourt, Francia, +33 1 41 86 10 00