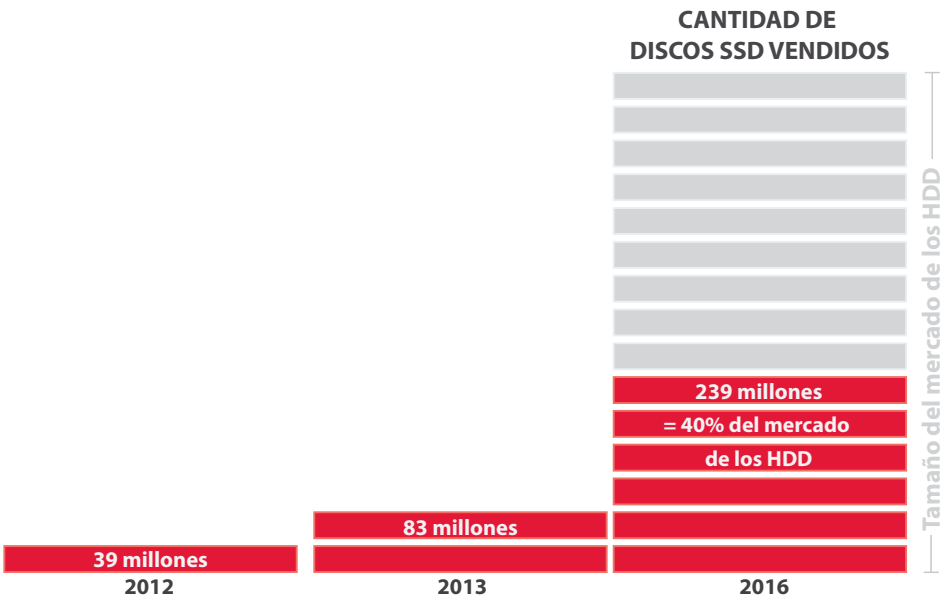
blancco
CERTIFIED DATA ERASURE

Retos y soluciones para el borrado de datos eficaz de SSD

Un libro blanco de Blancco

Publicado el 8 de octubre de 2013
Primera edición

Índice



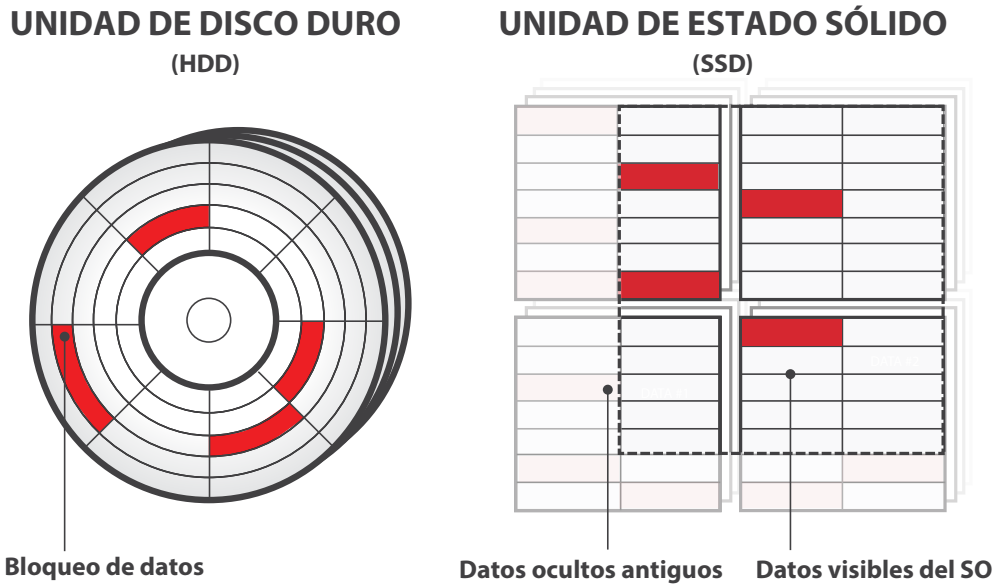
Introducción

El versátil y fiable dispositivo de almacenamiento masivo, el SSD (Solid State Drive) ha pasado de ser un producto especializado a un artículo de consumo mayoritario y uso empresarial, funcionando como el sustituto directo de la unidad de disco duro (HDD) tradicional. Gracias al rendimiento mejorado, fiabilidad y tamaño reducido del SSD, se estima que los envíos de SSD alcancen alrededor de lo 83 millones de unidades en 2013, lo que supone un aumento de más del 100% en las ventas de estas unidades durante 2012.[1]

A medida que aumenta la popularidad de los SSD, los responsables de los activos de TI y los especialistas de eliminación de activos de TI (ITAD por sus siglas en inglés) se enfrentan a varios retos relacionados con el borrado seguro de los grupos de SSD para su retirada, reasignación o eliminación. A diferencia de su equivalente disco mecánico, el HDD, un SSD emplea memoria flash lo que complica la eliminación total de los datos usando los métodos establecidos para los HDD.

Además, debido a que el mercado de los SSD ha crecido tan rápidamente, se ha producido una saturación con un elevado número de vendedores, cada uno de los cuales tiene su propia gama de modelos de SSD que además suelen ser diferentes en cuando a sus procesos operativos. Esta falta de estandarización complica aún más el borrado, especialmente dada la velocidad a la que siguen evolucionando los SSD.

Para los responsables de activos de TI de las empresas, así como para los recicladores externos y los ITAD que les asisten, es importante comprender la tecnología SSD, por qué el borrado de SSD es todo un reto y la importancia de elegir un producto de borrado eficaz con capacidades de creación de informes detallados. El software de borrado de datos eficaz y eficiente es desarrollado por un proveedor que puede aplicar técnicas diseñadas exclusivamente para borrar los SSD, así como conseguir la verificación por parte de terceros de la eficacia del software de borrado, ofreciendo a la vez acceso a importantes recursos de I+D para seguir el ritmo de esta tecnología emergente. Esta especialización evita que se produzcan falsos positivos debido al uso de una tecnología o proceso de borrado ineficaz lo que podría causar una costosa pérdida de información.

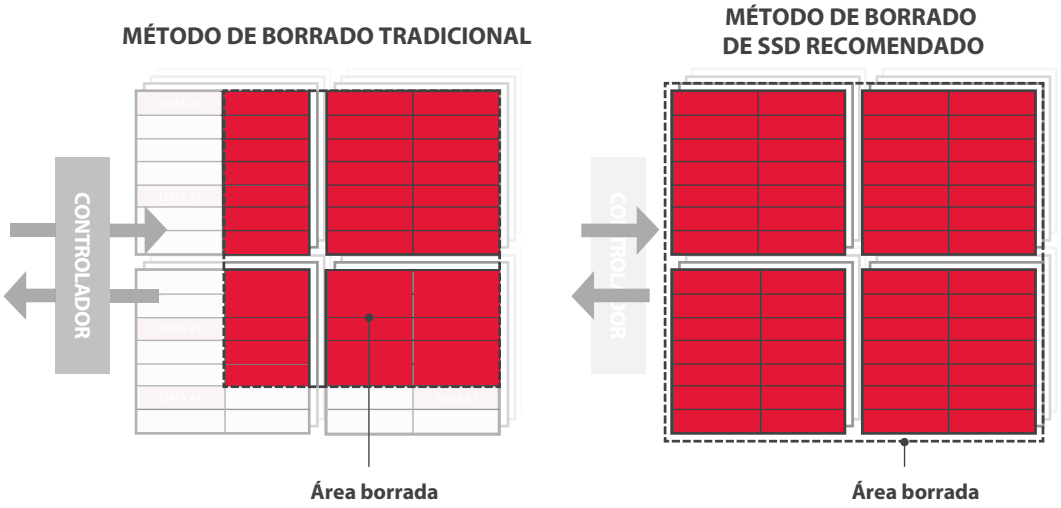


La simplicidad y la complejidad de los SSD

Desde un punto de vista físico, los SSD son simples en el sentido de que no contienen piezas móviles mecánicas, a diferencia de los HDD, que tienen discos que giran y cabezales de lectura/escritura móviles. En comparación, los SSD son más pequeños, más silenciosos, más rápidos y menos susceptibles de un fallo físico. Los SSD tienen un tamaño de aproximadamente la mitad de un disco duro, pesan como mucho la mitad y utilizan la mitad de energía, lo que los hace especialmente adecuados para los centros de datos y otros entornos de almacenamiento masivo.

Pero desde otra perspectiva, los SSD son cada vez más complejos. La memoria flash, similar a la que utilizan los SSD, se ha empleado durante años en las unidades USB, los reproductores de música portátiles, los teléfonos móviles y las tarjetas de memoria, entre otros. Sin embargo, la forma de gestionar los datos en estos «dispositivos simples» se diferencia en varios aspectos si la comparamos con los procesos realizados por un SSD y su controlador de memoria flash.

Los chips de memoria interna de los SSD – denominados flash NAND – son muy similares a los que se encuentran en otros dispositivos; la diferencia radica en que un SSD aplica esquemas de gestión de datos complejos para distribuir los datos por la memoria. Los SSD contienen además un conjunto mucho mayor de capacidad de memoria extra (libre) a la que sólo puede acceder el SSD. Son necesarios estos y otros procesos para prolongar el rendimiento y la vida útil de la unidad que son las ventajas principales de los SSD. Sin embargo, están ocultos en la vista del ordenador host y por lo tanto, del usuario. Todas estas diferencias separan a los SSD del resto de almacenamiento basado en flash y plantean la necesidad de un método distinto para borrarlos.



Los métodos de borrado tradicional suponen riesgos para los SSD

Debido a las diferencias en el funcionamiento de la memoria flash en los SSD, su borrado conlleva requisitos adicionales si lo comparamos con los teléfonos móviles, las unidades USB y otros dispositivos más sencillos. Los requisitos de borrado de SSD también se diferencian mucho de los del borrado de HDD, que se habían realizado eficazmente mediante software durante muchos años.

Existe varios métodos para el borrado de datos en los SSD, pero cada uno conlleva sus propios factores de riesgo:
Los **comandos Eliminar/Formatear** no son eficaces como medio de saneamiento de un SSD ya que existe la posibilidad de que los datos permanezcan en el dispositivo, que puede ser recuperable por expertos forenses de recuperación de datos.

La **destrucción física** deja la unidad inoperativa y elimina por tanto, la oportunidad de una recuperación de la inversión o de demostrar prácticas sostenibles y respetuosas con el medio ambiente. Y lo que es más importante, la destrucción inadecuada de los SSD puede ofrecer oportunidades a sus adversarios más cualificados de recuperar datos de sus fragmentos de chip flash.[2]

El **desmagnetizado** funciona bien con los HDD, pero los SSD utilizan circuitos integrados para almacenar los datos y estos circuitos se programan y se eliminan eléctricamente. Por tanto, los datos almacenados en la memoria flash NAND de un SSD no se ven afectados por la aplicación de un campo magnético.

La **sobrescritura de datos** en un SSD utilizando los estándares diseñados para los HDD como DoD 5220.22-M o HMG presenta problemas potenciales con la eliminación fiable de todos los datos del usuario. Esto se debe a las propiedades específicas de un SSD y cómo gestiona los datos en un dispositivo – una afirmación respaldada por resultados empíricos.[3]

Las técnicas de **borrado basado en firmware** como el Borrado seguro de ATA no son fiables de forma universal para los SSD. Esto se debe a que los fabricantes de SSD no han adoptado un método estandarizado para el borrado de datos.[4]

El **borrado criptográfico** «sanea» un disco a través de la modificación de la clave utilizada para encriptar/desencriptar datos, pero los datos siguen permaneci-

endo de forma efectiva en el dispositivo, por lo que son susceptibles de una implementación indebida del sistema criptográfico. Pueden surgir problemas al intentar verificar el borrado.

El **Borrado selectivo** puede ser necesario en diferentes fases del ciclo de vida de un SSD para sanear de forma segura los archivos individuales de una unidad. Sin embargo, los controladores de SSD tienden a escribir los datos en nuevas ubicaciones, en lugar de «en su sitio», lo que dificulta garantizar que también se han eliminado todas las copias obsoletas.

Factores externos que complican el borrado de SSD

Además de las complejidades técnicas internas, existen factores externos que exigen a aquellos que necesitan borrar los SSD que elijan un proveedor capaz de aplicar técnicas de borrado de datos eficaces. Estos factores son, entre otros, las variaciones de los fabricantes en la tecnología, junto con los requisitos legales y reglamentarios.

Falta de estandarización de los OEM (fabricantes de equipos originales)

La rápida adopción de los SSD ha tenido como resultado que un gran número de fabricantes de equipos originales (OEM) de SSD quiera participar en este mercado emergente. Con tantos OEM en el mercado a la vez, existe una falta de estandarización en los elementos que rodean a la tecnología SSD. La aceptación de criterios por todo el sector, incluidos los métodos de borrado de datos, ha sido algo tardío.[5]

Elegir un proveedor de borrado de datos con tecnología que ofrezca informes detallados y un certificado de borrado resulta crítico para cumplir con las leyes y normas en todo el mundo.

La variedad de modelos de SSD con sus variaciones en el hardware y en los procesos, se suma a la complejidad de elegir el mejor método para la gestión de soluciones de final de ciclo de vida útil. No es posible asumir que el comportamiento de un SSD concreto coincidirá con el siguiente, por lo que los conocimientos y especialización de un proveedor de software de borrado resultan críticos.

Aumento de la legislación y normas relativas a la privacidad de datos

La privacidad y la protección de datos es un asunto en desarrollo y existen muchas normas y reglamentos estrictos específicos del sector para proteger los datos. Al mismo tiempo, se implementan nuevas leyes. En 2012, los EE.UU. introdujeron la Declaración de derechos de privacidad del consumidor[6] que establece una fuerte protección de la privacidad de los consumidores, incluido el requisito de eliminación de datos.

En Europa, se han propuesto modificaciones en la protección de datos, que incluyen requisitos para la eliminación de los datos en línea, el uso de procedimientos auditables y recomendaciones para el uso de herramientas de borrado de datos certificadas.[7] Los infractores pueden incurrir en multas de hasta un 2% de su facturación anual total.

Aunque las leyes y las normas pueden variar entre países y sectores, siempre existe un requisito común: debe existir una prueba verificable del borrado de datos. Elegir un proveedor de borrado de datos con tecnología que ofrezca informes detallados y un certificado de borrado resulta crítico para cumplir con las leyes y normas en todo el mundo.

Requisitos principales para el borrado seguro de SSD

Las empresas y las organizaciones dependen de los procesos presentados por las compañías profesionales de borrado de datos para ofrecer seguridad para sus datos. Si no se es consciente de los retos que presentan los SSD se producirá un aumento de las posibilidades de una infracción. Existen algunos requisitos clave que el software de borrado profesional debe cumplir para garantizar el borrado de datos correcto de los SSD.

Comprobación y validación por terceros

Al desarrollar un proceso de borrado de SSD, resulta esencial para el proveedor de software contar con un tercero independiente experto en informática forense y recuperación de datos para que verifique y analice sus procesos de borrado de datos. Esta es la forma más eficaz e imparcial de determinar la solidez de un proceso de borrado. Sólo aquellos proveedores de borrado de datos con tecnología que superen estas estrictas y reconocidas pruebas forenses podrán afirmar de forma definitiva que pueden ofrecer una solución eficaz para borrar los SSD y otras tecnologías emergentes.

Los proveedores de borrado de SSD deben buscar todos los sistemas de validación disponibles para validar su solución de forma independiente. La Alianza para la eliminación de activos y seguridad de la información (ADISA por sus siglas en inglés) ha desarrollado una metodología diseñada para probar el software de saneamiento para SSD.[8] Las pruebas, llevadas a cabo por expertos en seguridad, verifican el borrado de SSD con los requisitos de un conjunto definido de normas forenses.

Para evaluar el proceso de borrado siguiendo las tácticas conocidas más avanzadas del sector, los procesos de borrado también deben probarse utilizando los

Al desarrollar un proceso de borrado de SSD, resulta esencial para el proveedor de software contar con un tercero independiente experto en informática forense y recuperación de datos para que verifique y analice sus procesos de borrado de datos.

conocimientos especializados de los expertos de recuperación de datos de primera categoría. Las compañías de recuperación de datos con años de experiencia y las herramientas de recuperación personalizadas que han desarrollado internamente puede proporcionar los procesos más exactos para juzgar el éxito del borrado.

El software de borrado de datos avanzado debe aplicar métodos automatizados para eliminar los bloqueos de inmovilización y garantizar que los métodos esenciales de borrado de firmware están accesibles.

En busca de la estandarización del borrado de SSD

El software de borrado debe aplicar técnicas de borrado diseñadas específicamente para proporcionar la mejor seguridad posible. De forma ideal, el software debe incorporar un estándar de borrado de SSD que requiere procesos de borrado que tengan la capacidad de contrarrestar las particularidades específicas del SSD, así como la posibilidad de mostrar todas las medidas de seguridad disponibles en una unidad. Las investigaciones publicadas ya han demostrado que la confianza en un método de borrado específico no es recomendable ni adecuado de forma universal para los SSD.[9]

Este estándar de borrado de SSD debe ofrecer un método de borrado multicapa, capaz de detectar los fallos de la unidad y de realizar la verificación más estricta posible. Los procesos realizados en un SSD deben incluir elementos que están diseñados para evitar los falsos positivos que estas unidades pueden comunicar al informar del éxito del borrado.

Eliminación de los bloqueos de inmovilización

Un aspecto fundamental del borrado de SSD correcto es conseguir el acceso a los comandos de borrado internos del dispositivo. La BIOS de la mayoría de los ordenadores modernos bloquea el acceso a estos comandos a través de la aplicación de un bloqueo en el conjunto de funciones de seguridad de la unidad (denominado «bloqueo de inmovilización»). La existencia de bloqueos de inmovilización puede suponer un importante reto para el borrado seguro y eficaz de los SSD, ya que la única forma de eliminar un bloqueo de inmovilización suele ser el acceso físico al disco duro.

Debido a que los SSD aplican el uso de áreas de almacenamiento a las que no se puede acceder mediante el software, las técnicas de borrado basadas en firmware son críticas a la hora de garantizar el proceso de saneamiento. Sin embargo, sin acceso a la eliminación automática del bloqueo de inmovilización este proceso se dificulta mucho. Tener acceso físico al SSD es poco práctico y resulta ineficaz en entornos en los que se procesan grandes volúmenes de activos, que necesitan más tiempo y esfuerzo para realizar las operaciones, especialmente en los portátiles en los que el acceso al SSD es difícil y requiere mucho tiempo. Además existe la posibilidad de errores e incluso de dañar la tecnología por un uso inadecuado.

El software de borrado de datos avanzado debe aplicar métodos automatizados para eliminar los bloqueos de inmovilización y garantizar que los métodos esenciales de borrado de firmware están accesibles.

Cooperación entre proveedor y OEM

La actual falta de estandarización alrededor de los SSD indica la necesidad para los proveedores de borrado y los fabricantes (OEM) de SSD de cooperar en la creación de una base de conocimientos eficaz en relación a la funcionalidad de SSD. Estos tipos de colaboraciones garantizan que se adopten las mejores prácticas de borrado para que las funciones de seguridad de los OEM estén accesibles y se realicen adecuadamente.

La cooperación continuada implica además que los proveedores de borrado de datos pueden actuar como terceros para validar los procesos de borrado internos de los OEM y garantizar que cumplen los más elevados requisitos de seguridad.

Resumen: Las herramientas profesionales superan las barreras del borrado de los SSD

En el futuro, los SSD serán una alternativa de almacenamiento aún más predominante tanto para los consumidores como para las empresas, con un mayor impacto en la dinámica del sector del borrado de datos. Para cumplir las sólidas políticas y prácticas de seguridad de datos es necesario que los responsables de activos de TI y los ITAD comprendan las diferencias entre los requisitos de borrado de datos de los HDD y los SSD para que puedan elegir una herramienta de borrado eficaz, especialmente a medida que la tecnología SSD continúa desarrollándose.

Al seleccionar una herramienta de borrado de datos que pueda procesar de forma eficaz los SSD, es esencial buscar una desarrollada por un proveedor que comprenda las numerosas exigencias que implica la tecnología SSD. En caso contrario, podría utilizarse una herramienta o método de borrado menos avanzado, lo que presentaría una potencial pérdida de información y eliminaría la posibilidad de disfrutar de lucrativas oportunidades de reventa.

El software de borrado de datos profesional elimina las barreras para borrar mediante la superación de los bloqueos de inmovilización, la detección de errores en la unidad y la creación de informes de la incapacidad del SSD para cumplir de forma eficaz las operaciones de borrado de forma que puedan utilizarse procedimientos alternativos para eliminar riesgos. El informe de borrado exhaustivo del software también permite el cumplimiento de las distintas reglamentaciones y normas y ofrece los detalles de hardware necesarios para la reventa del dispositivo. Por último, el software de borrado de datos avanzado proporciona la tranquilidad de que los datos confidenciales no caerán en las manos inadecuadas.

Referencias

[1] Zhang, Fang, IHS iSuppli, «Hard Disk Drive Market Revenue Set for Double-Digit Decline This Year», 4 de febrero de 2013, www.isuppli.com/Memory-and-Storage/News/Pages/Hard-Disk-Drive-Market-Revenue-Set-for-Double-Digit-Decline-This-Year.aspx

[2] Swanson, Steven, «Destroying Flash Memory-Based Storage Devices» University of California, San Diego, CA, 2011, cseweb.ucsd.edu/users/swanson/papers/TR-cs2011-0968-Grind.pdf

[3] Grupp L., Spada F., Swanson S., Wei M., «Reliably Erasing Data From Flash-based Solid State Drives», 2010

[4] Grupp et. al, 2010

[5] Belkasort, «Why SSD Drives Destroy Court Evidence, and What Can Be Done About It», forensic.belkasoft.com/en/why-ssd-destroy-court-evidence

[6] Obama Administration, «Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy», febrero de 2012, www.whitehouse.gov/sites/default/files/privacy-final.pdf

[7] European Commission, enero de 2012, ec.europa.eu/justice/data-protection/index_en.htm

[8] ADISA Product Claims Testing, www.adisa.org.uk/claimstesting/

[9] Grupp et. al, 2010

C. Anabel Segura 7, 28108 Alcobendas, Madrid
900 112 012, www.ontrackdatarecovery.es